



Recording Component (RC-L / RC-E)

User Manual

On-Net Surveillance Systems, Inc.
One Blue Hill Plaza, 7th Floor, PO Box 1555
Pearl River, NY 10965
Phone: (845) 732-7900 | Fax: (845) 732-7999
Web: www.onssi.com

0006302014-1311-RC-LE_7.0-O4.0.0.56

Legal Notice

This product manual is intended for general information purposes only, and due care has been taken in its preparation.

Any risk arising from the use of this information rests with the recipient, and nothing herein should be construed as constituting any kind of warranty.

© 2002-2014 On-Net Surveillance Systems, Inc. All rights reserved. OnSSI and the 'Eye' logo are registered trademarks of On-Net Surveillance Systems, Inc. Ocularis, Ocularis Client, Ocularis Client Lite, Ocularis Video Synopsis, NetEVS, NetDVMS, NetDVR, ProSight, NetGuard, NetGuard-EVS, NetSwitcher, NetMatrix, NetCentral, NetTransact, NetPDA and NetCell are trademarks of On-Net Surveillance Systems, Inc. All other trademarks are property of their respective owners.

On-Net Surveillance Systems, Inc. reserves the right to change product specifications without prior notice.

Contents

BEFORE YOU START	8
INTRODUCTION TO ONLINE HELP	8
NAVIGATE THE BUILT-IN HELP SYSTEM	8
SYSTEM OVERVIEW	9
PRODUCT OVERVIEW	9
SYSTEM COMPONENTS.....	9
Management server	9
Failover management server	9
Recording server.....	9
Failover recording server	10
Log server	10
SQL server.....	10
Active Directory.....	10
Virtual servers	10
Clients	11
ABOUT LICENSES.....	13
DIFFERENTIATE LS AND ES RECORDERS.....	13
ABOUT LOCAL IP ADDRESS RANGES	14
SYSTEM REQUIREMENTS	14
INSTALLATION.....	15
INSTALLATION PRECONDITIONS	15
Determine installation method.....	15
Determine SQL server type.....	15
Select service account	16
Active Directory.....	16
Customize IIS.....	16
About virus scanning.....	17
INSTALL THE SYSTEM	17
Install your system - Single Server option	18
Install your system - Distributed option	18
Install your system - Custom option	19
Install the recording server.....	20
Installation for workgroups	20
Installation troubleshooting	21
CONFIGURE THE SYSTEM IN MANAGEMENT CLIENT	22
Change Software License Code	23
RECORDER DOWNLOADS WEB PAGE	24
UPGRADE	24
About upgrades.....	24
Upgrade prerequisites.....	25
Alternative upgrade for workgroup	25
FIRST TIME USE.....	26
BEST PRACTICES.....	26
Protect recording databases from corruption	26
About daylight saving time	26
About time servers	27
MANAGEMENT CLIENT OVERVIEW.....	27
About login authorization	27
Management Client window	27
Panels overview.....	27
Menu overview	28
MANAGEMENT CLIENT ELEMENTS.....	30
BASICS.....	30

License information	30
Site information	32
SERVICES AND HARDWARE	33
Recording servers	33
Hardware and remote servers	45
Remove a recording server	51
Delete all hardware on a recording server	51
DEVICES	52
Working with device groups	52
Working with devices	54
CLIENT	77
About clients	77
View groups	77
Management Client profiles	78
NetMatrix	80
RULES AND EVENTS	81
About rules and events	81
About actions and stop actions	82
Events overview	87
Rules	91
Time profiles	97
Notification profiles	100
User-defined events	103
SECURITY	104
Roles	104
Basic users	120
SYSTEM DASHBOARD	121
About system dashboard	121
About system monitor	121
About current tasks	122
About configuration reports	122
SERVER LOGS	123
About logs	123
Search logs	124
Export logs	124
Change log language	124
System log properties	124
Audit log properties	125
Rule log properties	126
OPTIONS DIALOG BOX	126
General tab (options)	127
Server Logs tab (options)	128
Mail Server tab (options)	129
AVI Generation tab (options)	129
Network tab (options)	130
User Settings tab (options)	130
FAILOVER CONFIGURATION	131
FAILOVER RECORDING SERVERS (REGULAR AND HOT STANDBY)	131
About failover recording servers	131
About failover steps	132
About failover recording server functionality	133
Install a failover recording server	133
Setup and enable failover recording servers	134
Assign failover recording servers	134
Group failover recording servers	135
Read failover recording server status icons	136
Failover recording server properties	136
Failover group properties	136
About failover recording server services	137
View status messages	137
Change the management server address	137

View version information	137
FAILOVER MANAGEMENT SERVERS	138
About multiple management servers (clustering)	138
Prerequisites for clustering	138
Install in a cluster	138
Upgrade in a cluster	139
REMOTE CONNECT SERVICES	140
About remote connect services	140
Install STS environment for One-click camera connection	140
Add/edit STSs	140
Register new Axis One-click camera	141
Axis One-Click Camera connection properties	141
ONSSI FEDERATED ARCHITECTURE	142
About selecting Interconnect or OnSSI Federated Architecture	142
About OnSSI Federated Architecture	142
Set up your system to run federated sites	143
Add site to hierarchy	144
Accept inclusion in hierarchy	144
Refresh site hierarchy	145
Connect to another site in hierarchy	145
Detach a site from the hierarchy	145
Federated site properties	146
INTERCONNECT	146
About selecting Interconnect or OnSSI Federated Architecture	146
About Interconnect	147
About possible Interconnect setups	148
Interconnect and licensing	148
Update remote site hardware	148
Establish remote desktop connection to remote system	149
Enable playback directly from remote site camera	149
Retrieve remote recordings from remote site camera	149
MULTI-DOMAIN WITH ONE-WAY TRUST	150
Setup with one-way trust	150
SNMP	150
About SNMP support	150
Install SNMP service	151
Configure SNMP service	151
OCULARIS CS SERVERS	151
About Ocularis CS servers	151
Add Ocularis CS servers	152
Define roles with access to Ocularis CS servers	152
Edit Ocularis CS servers	152
SYSTEM MAINTENANCE	153
PORTS USED BY THE SYSTEM	153
BACKING UP AND RESTORING CONFIGURATION	154
About backing up and restoring your system configuration	154
Back up log server database	155
Manual backup and restore	155
Scheduled backup and restore	156
MOVING THE MANAGEMENT SERVER	158
About moving the management server	158
About unavailable management servers	159
Move the system configuration	159
MANAGING THE SQL SERVER	159
About updating the SQL server address	159
Update the log server's SQL address	159
REPLACE HARDWARE	160
REPLACE A RECORDING SERVER	161
VIDEO DEVICE DRIVERS	161
About video device drivers	161
About removing video device drivers	162

SERVICES.....	162
About the Management Server service and Recording Server service.....	162
View status messages	162
Read server service icons - management, recording and failover	163
Change recording server settings	163
Recording server properties.....	164
REGISTERED SERVICES.....	164
About the service channel.....	164
Add and edit registered services.....	165
Manage network configuration.....	165
Registered services properties.....	166
INDEX	167

Copyright, trademarks and disclaimer

Copyright

© 2014 On-Net Surveillance Systems, Inc.

Trademarks

is a registered trademark of On-Net Surveillance Systems, Inc..

Microsoft and Windows are registered trademarks of Microsoft Corporation. App Store is a service mark of Apple Inc. Android is a trademark of Google Inc.

All other trademarks mentioned in this document are trademarks of their respective owners.

Disclaimer

This text is intended for general information purposes only, and due care has been taken in its preparation.

Any risk arising from the use of this information rests with the recipient, and nothing herein should be construed as constituting any kind of warranty.

On-Net Surveillance Systems, Inc. reserve the right to make adjustments without prior notification.

All names of people and organizations used in the examples in this text are fictitious. Any resemblance to any actual organization or person, living or dead, is purely coincidental and unintended.

This product may make use of third party software for which specific terms and conditions may apply. When that is the case, you can find more information in the file *3rd_party_software_terms_and_conditions.txt* located in your OnSSI surveillance system installation folder.

Before you start

Introduction to Online help

Online help is divided into sections that each serves a targeted purpose. The sections are structured in a logical flow:

System overview (on page 9)

Provides an introduction to your video surveillance system, system components, and concepts. This is useful if you are new to the system. The system overview also provides a comparison chart that lists the most significant differences between Ocularis ES and Ocularis LS.

Installation (on page 15)

Provides installation preconditions and step by step procedures that help you install and upgrade your system.

First time use (on page 26)

Provides an overview of the Management Client and information about best practices to follow to have your system running smoothly. This overview is useful if you are new to the system.

Management Client elements (on page 30)

Provides a thorough walk through of each of the nodes in the Site Navigation pane of the Management Client. This section contains conceptual and procedural information about the basic elements of your system.

Feature configuration (on page 131)

Provides self-contained, detailed information about the additional features and add-on products that your system supports.

System maintenance (on page 153)

Provides an overview of the ports used in the system and step-by-step procedures for, for example, backing up your system and monitoring system performance. This section is useful after installation and configuration in order to maintain, expand and optimize your system.

Navigate the built-in help system

Press F1 to access a related help topic or select **Help** > *Contents* from the Management Client toolbar to launch the complete help.

You can navigate between the help window's three tabs:

Tab	Description
Contents	Navigate the help system based on a tree structure.
Index	Select the first letter of the term you are interested in and scroll until you find it. Click a help topic title in the search results list to open the required topic.
Search	Search for help topics that contain particular terms of interest. For example, search for the term <i>zoom</i> and receive a list in the search result of all help topics that contains the term <i>zoom</i> . Click a help topic title in the search results list to open the required topic.

To print a help topic, navigate to the required topic and click the browser's *Print* button.

System overview

Product overview

This system is a fully distributed solution, designed for large multi-site and multiple server installations requiring 24/7 surveillance, with support for devices from different vendors. The solution offers centralized management of all devices, servers, and users, and empowers an extremely flexible rule system driven by schedules and events.

Your system consists of the following main elements:

- The **management server** - the center of your installation, consists of multiple servers
- One or more **recording servers**
- One or more **Management Clients**
- The **Download Manager**
- One or more **Ocularis Clients**.

Your system installation can take place on virtualized servers or on multiple physical servers in a distributed setup.

The system also offers the possibility of including the standalone Ocularis Viewer when you export video evidence from the Ocularis Client. Ocularis Viewer allows recipients of video evidence (such as police officers, internal or external investigators, etc.) to browse and play back the exported recordings without having to install any software on their computers.

The system supports an unlimited number of cameras, servers, and users and across multiple sites if required. .

System components

Management server

The management server stores the configuration of the surveillance system in a relational database, either on the management server computer itself or on a separate SQL Server on the network. It also handles user authentication, user rights, the rule system and more. To improve system performance, you can run several management servers in a Federated environment. The management server runs as a service, and is typically installed on a dedicated server.

Users connect to the management server for initial authentication, then transparently to the recording servers for access to for video recordings, etc.

Failover management server

Failover support on the management server is achieved by installing the management server in a Microsoft Windows Cluster. The cluster will then ensure that another server take over the management server function should the first server fail.

Recording server

The recording server is responsible for communicating with the network cameras and video encoders, recording the retrieved audio and video as well as providing client access to both live and recorded audio and video.

Device Drivers

- Communication with the network cameras and video encoders are done through a device driver developed specifically for individual devices or a series of similar devices from the same manufacture.
- The device drivers are installed by default when the recording server is installed, but can later be updated by downloading and installing a newer version of the device pack.

Media Database

- The retrieved audio and video data is stored in a high performance media database optimized for recording and storing audio and video data.
- The media database supports various unique features like; multistage archiving, video grooming, encryption and adding a digital signature to the recordings.

Failover recording server

For RC-E, the failover recording server is responsible for taking over the recording task should a recording server fail.

The failover recording server can operate in two modes:

- Standard failover – for monitoring multiple recording servers
- Hot-standby – for monitoring a single recording server

The difference between the standard and hot-standby failover modes is that in the standard failover mode the failover recording server does not know which server to take over from, so it cannot start until a recording server fails. In the hot-standby mode the failover time is significantly shorter, as the failover recording server already knows which recording server it should take over from and thus can pre-load the configuration and start up completely - except for the last step of connecting to the cameras.

Log server

The log server is responsible for storing all log messages for the entire system. The log server uses the same SQL server as the management server and is typically installed on the same server as the management server, but can be installed on a separate server if needed to increase performance of the management and log servers.

SQL server

The management server and log server uses an SQL server to store, for example, the configuration, alarms, events and log messages.

The system installer includes Microsoft SQL Server 2008 R2 Express that can be used freely for systems up to 300 cameras.

For larger systems over 300 cameras it is recommended to use the SQL Server 2008 R2 Standard or Enterprise edition on a dedicated server as these editions can handle larger databases and offer backup functionality.

Active Directory

You normally add users from Active Directory, but you can also add users without Active Directory. Active Directory is a distributed directory service included with several Windows Server operating systems. It identifies resources on a network in order for users or applications to access them.

Virtual servers

You can run all system components on virtualized Windows® servers, such as VMware® and Microsoft® Hyper-V®.

Virtualization is often preferred to better utilize hardware resources. Normally, virtual servers running on the hardware host server do not load the virtual server to a great extent, and often not at the same time. However, recording servers record all cameras and video streams. This puts high load on CPU, memory, network, and storage system. So, when run on a virtual server, the normal gain of virtualization disappears to a large extent, since - in many cases - it uses all available resources.

If run in a virtual environment, it is important that the hardware host has the same amount of physical memory as allocated for the virtual servers and that the virtual server running the recording server is allocated enough CPU and

memory - which it is not by default. Typically, the recording server needs 2-4 GB depending on configuration. Another bottleneck is network adapter allocation and hard disk performance. Consider allocating a physical network adapter on the host server of the virtual server running the recording server. This makes it easier to ensure that the network adapter is not overloaded with traffic to other virtual servers. If the network adapter is used for several virtual servers, the network traffic might result in the recording server not retrieving and recording the configured amount of images.

Clients

About the Management Client

Feature-rich administration client for configuration and day-to-day management of the system. Available in several languages.

Typically installed on the surveillance system administrator's workstation or similar.

For a detailed overview of the Management Client, see Management Client overview (on page 27).

About Ocularis Client

Designed for the Ocularis video management software, the Ocularis Client is an easy-to-use client application that provides intuitive control over security installations.

Ocularis Client allows users to:

- Monitor live video from an unlimited number of cameras at multiple sites with instant investigation capabilities
- Easily access and investigate alerts generated by motion detection, external systems and events configured by the administrator
- Export video clips and still images for further event handling or as court evidence
- Organize alerts into incident cases using the Alert Manager interface
- Be alerted to events with Blank Screen Monitoring and audible sounds
- Bookmark exported video clips for sharing and easy retrieval
- Monitor the surveillance environment in command centers with Video Wall support
- Maintain situational awareness with Critical Camera Failover

These and many more features are found in the free Ocularis Client application.

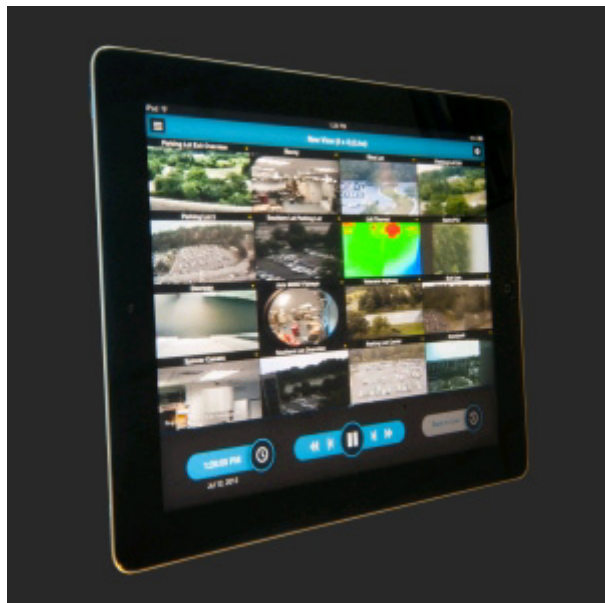
Ocularis Client must be installed on users' computers. Surveillance system administrators manage clients' access to the surveillance system through the Ocularis Administrator application. Recordings viewed by clients are provided by the recorder's Image Server service. The service runs in the background on the surveillance system server. Separate hardware is not required.

To download Ocularis Client, connect to the Ocularis Base system server which presents you with an Ocularis components download page. For more details, see the *Ocularis Installation and Licensing Guide*.

About Ocularis Mobile

With Ocularis Mobile you can mobilize 16 HD streams on iPad tablets and iPhone devices at full frame rate and full resolution. Ocularis Mobile brings the true experience of video surveillance to your mobile devices.

For a complete list of features and supported devices, see our website at: <http://www.onssi.com/products/add-ons>



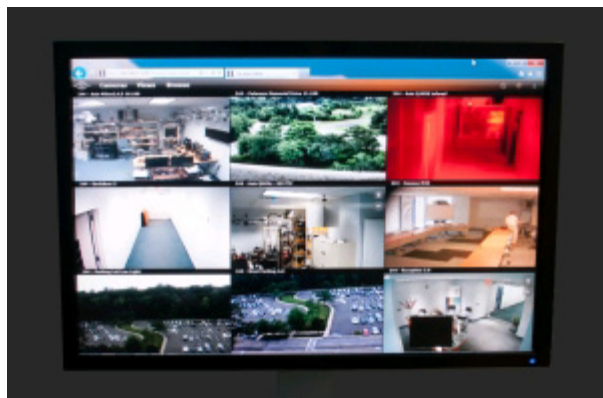
If you want to use Ocularis Mobile with your system, you must add an Ocularis Media Server to establish the connection between the mobile client and your system. Download Ocularis Mobile for free from corresponding app stores.

About Ocularis Web

Ocularis Web is a web-based client application for viewing, playing back and sharing video. It provides instant access to the most commonly used surveillance functions, such as viewing live video and play back of recorded video

Features include: support for up to 16 HD/megapixel video streams displayed at full framerate (30 fps), toggle each camera between full-screen and grid view, access recorded video using timeline, support for any combination of image resolutions (megapixel, HD and SD) and compression formats (MJPEG, MxPEG, MPEG4, H.264) and support for all standard web browsers. For a full list of features and requirements, see our website at <http://www.onssi.com/products/add-ons>.

Access to features depends on individual user rights which are set up in the Ocularis Administrator.



To enable access to Ocularis Web, you must install an Ocularis Media Server. Ocularis Web itself does not require any installation and works with most Internet browsers. Once you have set up Ocularis Media server, you can monitor the system anywhere from any supported browser (provided you know the proper credentials).

About licenses

When you purchase the system, you also purchase software licenses for the cameras/devices used. One license is associated with one IP address. For each single-lens IP camera, you need one license. In the case of multi-lens cameras, such as an Arecont or Axis area view camera, where there are multiple streams but only one IP address, only one license is required. For video encoders, if the encoder has one IP address with multiple ports/channels, you still only need one software license even though you may stream multiple cameras through this device. If the encoder has one IP Address for each channel, then one license is required for each.

At first, when you have installed the various system components, configured the system, and added recording servers and cameras through the Management Client, the surveillance system runs on temporary licenses which need to be activated before a certain period ends. This is known as the grace period. You also need to activate licenses if you later add more cameras to the system.

When the new surveillance system is working, OnSSI recommends that you activate your licenses before you make the final adjustments. If you do not activate your licenses before the grace period expires, all recording servers and cameras without activated licenses stop sending data to the surveillance system.

Differentiate LS and ES Recorders

This help system supports two similar recording components for:

- Ocularis LS
- Ocularis ES

The recording component names are: RC-L and RC-E respectively.

Below is a list of the differences between the two recorders:

Name	RC-L	RC-E
Interconnect	Remote site	Central/remote site
OnSSI Federated Architecture	Remote site	Central/remote site
Recording server failover and hot stand-by recording server	-	✓
Remote connect services	-	✓
Multi-stage video storage	Ocularis ES database Live databases + 1 archive	Ocularis ES database Live databases + unlimited archives
Reduce frame rate (grooming)	-	✓
Video data encryption (recording server)	-	✓
Database signing (recording server)	-	✓
SNMP trap (notification)	-	✓

About local IP address ranges

When a client, such as Ocularis Client, connects to a surveillance system, an amount of initial data communication occurs in the background. This happens automatically, and is transparent to users.

Clients may connect from the local network as well as from the Internet, and in each case the surveillance system should be able to provide suitable addresses so the clients can get access to live and recorded video from the recording servers:

- When clients connect locally, the surveillance system should reply with local addresses and port numbers.
- When clients connect from the Internet, the surveillance system should reply with the recording servers' public addresses, that is the address of the firewall or NAT (Network Address Translation) router, and often also a different port number (which is then forwarded to recording servers).

The surveillance system must therefore be able to determine whether a client belongs on a local IP range or on the Internet. For this purpose, you can define a list of IP ranges which the surveillance system should recognize as coming from a local network.

System requirements

Important: The recording component is no longer supported on Microsoft® Windows® 2003 (however, you can still run other components from computers with Windows 2003).

Important: The recording component is no longer supported on Microsoft® Windows® 32-bit OS (however, you can still run other components from computers with Windows 32-bit OS).

For information about the *minimum* system requirements to the various components of your system, go to <http://www.onssi.com/hardware-recommendations> <http://www..>

Installation

If you upgrade from a previous version, see About upgrade (on page 24).

Installation preconditions

Read the installation preconditions before you start the actual installation.

Determine installation method

As part of the installation wizard, you must decide which installation method to use. Your selection depends on the organization needs, but has typically been determined when purchasing the system.

The options are:

- **Single Server:** installs all management server components and recording server on the current computer. You only need to make a minimum of selections and all components are preselected in the un-editable component list. The SQL server is not in the list, but is also installed on the current computer.
- **Distributed:** installs only the management server components on the current computer. This means that the recording server is not visible in the un-editable component list. You must install the recording server and SQL server on other computers.
- **Custom:** allows you to select freely among all management server components and recording server to install on the current computer. By default, recording server is unselected in the component list, but you can edit this. Depending on your selections you must install the unselected component afterwards on other computers including the SQL server.

For easy user and group management, OnSSI recommends that you have Microsoft Active Directory® in place before you install your system. If you add the management server to the Active Directory after installing, you must re-install the management server, and replace users with new users defined in the Active Directory.

Determine SQL server type

Read the following information to determine which SQL server type is right for your organization:

The Microsoft SQL Server Express Edition is a "lightweight" version of a full SQL server. It is easy to install and prepare for use, and is often sufficient for systems with less than 300 cameras.

If you plan to perform frequent/regular backups of your database, OnSSI recommends using an existing SQL server on the network (you must have administrator rights on the SQL server).

For large installations (300 cameras or more), OnSSI recommends using a full-scale existing SQL server on a dedicated computer on the network.

OnSSI recommends that you install the database on a dedicated hard disk drive that is not used for anything else but the database. Installing the database on its own drive prevents low disk performance.

If you select **Distributed** or **Custom** as part of the installation wizard, you must decide what to do regarding the SQL server.

If you do not have an SQL server installed, the options are:

- **Install SQL Server 2008 Express on this computer.**
- **Use an existing SQL Server on the network:** When you use a dedicated computer for the SQL database on the network, the list of SQL servers that your account can access appears.

If you have an SQL server installed, the options are:

- **Use the installed Microsoft SQL Server Express database on this computer.**
- **Use an existing SQL Server on the network:** When you use a dedicated computer for the SQL database on the network, the list of SQL servers that your account can access appears.

You are also asked whether you want to create a new database, use an existing database, or overwrite an existing database.

- **Create new database:** For a new installation.
- **Use existing database:** If you are installing the database as part of upgrading to a newer version of the system, and you want to use your existing database.

Select service account

As part of the installation wizard, you are asked to specify the service account that will access the management server and the recording server to manage the services:

- With a predefined network service account (***This predefined user account***), the service always runs when the server (computer) are running - no matter which account is used. The account matters for access to various resources.
- With a particular user account (***This account***), the service uses the specified user account to run the service under the same account as the management server. If the server acting as management server is a member of a domain, you should either select the suggested **Network Service** or specify a user account for the domain.

If you use network drives, always specify a particular user account (with access to the network drives). Otherwise, the relevant service cannot access the required network drives.

Active Directory

If you want to add users through the Active Directory service, a server with Active Directory installed, and acting as domain controller, must be available on your network.

If you do not install Active Directory, follow Installation for workgroups (on page 20) when you start the installation.

Customize IIS

If you install on Windows Server 2008, OnSSI recommends that you customize the standard IIS installation:

1. In Windows *Start* menu, select *Control Panel*, then select *Programs and Features*.
2. In the *Programs and Features* window, click *Turn Windows features on or off*. This opens the *Windows Features* window (window name may be different depending on which operating system you are installing the service channel on).
3. In the *Windows Features* window, expand *Internet Information Services*.
4. Expand and select *Web Management Tools*, then expand and select *IIS 6 Management Compatibility*, then select *IIS Metabase and IIS 6 configuration compatibility*.
5. Expand and select *World Wide Web Services*, then expand and select *Application Development Features*, then select the following:
 - .NET Extensibility
 - ASP
 - ASP.NET
 - ISAPI Extensions
 - ISAPI Filters.
6. Expand and select *Security*, then select *Windows Authentication*.
7. Click *OK*.

About virus scanning

As is the case with any other database software, if an antivirus program is installed, it is important that you exclude specific file types and locations, as well as certain network traffic. Without implementing these exceptions, virus scanning uses a considerable amount of system resources. On top of that, the scanning process can temporarily lock files which likely results in a disruption in the recording process or even database corruption.

When you need to perform virus scanning, do not scan Recording Server directories containing recording databases (by default c:\mediadatabase\, as well as all folders under that location). Avoid also to perform virus scanning on archive storage directories. In older versions of the software, the databases are by default located in the installation folder, each being a subfolder with the MAC address of the device recorded.

Create the following additional exclusions:

- File types: .blk, .idx, .pic, .pqz, .sts, .ts
- C:\Program Files\OnSSI or C:\Program Files (x86)\OnSSI and all subdirectories.
- Exclude network scanning on TCP ports:

Product	TCP ports
RC-L and RC-E	80, 8080, 7563, 25, 21, 9993
RC-P, RC-I and RC-C	80, 25, 21, 1234, 1237, 22331
Ocularis Mobile	8081

or

- Exclude network scanning of the following processes:

Product	Processes
RC-L and RC-E	<i>VideoOS.Recording.Service.exe, VideoOS.Server.Service.exe, VideoOS.Administration.exe</i>
RC-P, RC-I and RC-C	<i>RecordingServer.exe, ImageServer.exe, ManagementApplication.exe, ImageImportService.exe, RecordingServerManager.exe, VideoOS.ServiceControl.Service.exe, VideoOS.Event.Server.exe</i>

Organizations may have strict guidelines regarding virus scanning, however it is important that the above locations and files are excluded from virus scanning.

Install the system

Select one of the installation options:

- Install your system - Single Server option (on page 18)
- Install your system - Distributed option (on page 18)
- Install your system - Custom option (on page 19)

Install your system - Single Server option

Download and launch the Recording Component from the Ocularis Download Components webpage located on the Ocularis Base computer (for further instructions, see the *Ocularis Installation and Licensing Guide*).

1. The installation files unpack. Depending on your security settings, one or more Windows security warnings appear. Accept these and the unpacking continues.
2. When done, the *RC-L / RC-E* dialog box appears,
 - a) Select the **Language** to use during the installation (this is **not** the language your system uses once installed, this is selected later). Click **Continue**.
 - b) In **Type the location of the license file**, enter the license file (.lic file). Alternatively, use the browse function to locate it. The system verifies your license file before you can continue. Click **Continue**.
 - c) Read the *OnSSI End-user License Agreement*. Select the **I accept the terms in the license agreement** check box.
3. Select **Single Server**. A list of components to install appears (you cannot edit this list). Click **Continue**.
4. Select **Files location** for the program file. In **Product language**, select the language in which the recording component should be installed. Click **Install**.
5. The software now installs. When done, you see a list of successfully installed components. Click **Close**.

Microsoft® IIS is automatically installed during the process. Afterwards, you may be prompted to restart your computer. Do so and after restart, depending on your security settings, one or more Windows security warnings may appear. Accept these and the installation completes.
6. When done, your installation completes and you can continue with configuration, see Configuration process (see "Configure the system in Management Client" on page 22).

Install your system - Distributed option

1. Download and launch the Recording Component from the Ocularis Download Components webpage located on the Ocularis Base computer (for further instructions, see the *Ocularis Installation and Licensing Guide*).
2. The installation files unpack. Depending on your security settings, one or more Windows security warnings appear. Accept these and the unpacking continues.
3. When done, the *RC-L / RC-E* dialog box appears,
 - a) Select the **Language** to use during the installation (this is **not** the language your system uses once installed, this is selected later). Click **Continue**.
 - b) In **Type the location of the license file**, enter the license file (.lic file). Alternatively, use the browse function to locate it. The system verifies your license file before you can continue. Click **Continue**.
 - c) Read the *OnSSI End-user License Agreement*. Select the **I accept the terms in the license agreement** check box.
4. Select **Distributed**. A non-editable list of components to be installed appears. Click **Continue**.
5. Select the type of SQL server database you want. Also specify the name of the SQL server. Click **Continue**.
6. Select either **Create new database** or **Use existing database** and name the database. If you choose the latter, select to **Keep** or **Overwrite** existing data. Click **Continue**.
7. Select **Files location** for the program file. In **Product language**, select the language in which the recording component should be installed. Click **Install**.
8. The software now installs. When done, you see a list of successfully installed components. Click **Close**.

Microsoft® IIS is automatically installed during the process. Afterwards, you may be prompted to restart your computer. Do so and after restart, depending on your security settings, one or more Windows security warnings may appear. Accept these and the installation completes.
9. Install the recording server on a separate computer, see Install the recording server (on page 20).

Install your system - Custom option

Note that with this option you can select or clear all of the components to install, except the management server. The management server is selected by default in the component list and is always installed. If one is already installed, it is updated.

Download and launch the Recording Component from the Ocularis Download Components webpage located on the Ocularis Base computer (for further instructions, see the *Ocularis Installation and Licensing Guide*).

1. The installation files unpack. Depending on your security settings, one or more Windows security warnings appear. Accept these and the unpacking continues.
2. When done, the *RC-L / RC-E* dialog box appears,
 - a) Select the **Language** to use during the installation (this is **not** the language your system uses once installed, this is selected later). Click **Continue**.
 - b) In **Type the location of the license file**, enter the license file (.lic file). Alternatively, use the browse function to locate it. The system verifies your license file before you can continue. Click **Continue**.
 - c) Read the *OnSSI End-user License Agreement*. Select the **I accept the terms in the license agreement** check box.
3. Select **Custom**. A list of components to be installed appears. Apart from the management server, all elements in the list are optional. The recording server is by default deselected, but you can change this if needed. Click **Continue**.
4. Select the type of SQL server database you want. If relevant, also specify the name of the SQL server. Click **Continue**.
5. Select either **Create new database** or **Use existing database** and name the database. If you choose the latter, select to **Keep** or **Overwrite** existing data. Click **Continue**.
6. Select either *This predefined account* or *This account* to select the service account. If needed, enter a password and confirm this. Click **Continue**.
7. If you have more than one available IIS website, you can select any of these. However, if any of your websites have HTTPS binding, select one of these. Click **Continue**.
8. Select **Files location** for the program file. In **Product language**, select the language in which the recording component should be installed. Click **Install**.
9. The software now installs. When done, you see a list of successfully installed components. Click **Close**.
Microsoft® IIS is automatically installed during the process. Afterwards, you may be prompted to restart your computer. Do so and after restart, depending on your security settings, one or more Windows security warnings may appear. Accept these and the installation completes.
10. Depending on your selections, install the remaining components on other computers:
 - a) Go to the Recorder download web page located on the Management Server. From a web browser, enter:
`http://<ip_address_of_management_server>/admin/installation/admin`
 - b) Select the link to install:
 - Recording Server
 - Management Client
 - Log server.
 - Axis One-click Connection Component
 - c) Run the installer.
11. Install the recording server on a separate computer, see Install the recording server (on page 20).

Install the recording server

Once you have installed the management server, download the separate recording server installer from the management server's web page.

See Install a failover recording server (on page 133) if you want to install a failover server.

1. Log into the computer where you want to install the recording server.
2. Open an Internet browser, and use the address of the Recorder Downloads web page from the management server:
`http://<ip_address_of_management_server>/installation/admin`
3. Select the Recording Server installer. Save the installer somewhere appropriate and run it from here or run it directly from the web page.
4. Select the **Language** you want to use during the installation. Click **Continue**.
5. Select:
Typical: to install a recording server with default values, or
Custom: to install a recording server with custom values.
6. Specify the recording server settings:
 - o Name.
 - o Management server address.
 - o Path to save recordings, and click **Continue**.
7. If you selected **Custom**:
 - a) Specify the number of recording servers you want to install on this computer. Click **Continue**.
 - b) Specify the service account. If needed, enter a password and confirm this. Click **Continue**.
8. Select **Files location** for the program file. In **Product language**, select the language in which to install your system. Click **Install**.
9. The software now installs. When done, you see a list of successfully installed components. Click **Close**.
When you have installed the recording server, you can check its state from the **Recording Server service** icon.
10. When done, your installation completes and you can continue with configuration, see Configuration process (see "Configure the system in Management Client" on page 22).

Installation for workgroups

If you do not use a domain setup with an Active Directory server, but a workgroup setup, do the following when you install:

1. Log in to Windows using a common administrator account.
2. Depending on your needs, start the management or recording server installation and click **Custom**.
3. Depending on what you selected in step 2, select to install the Management or Recording Server service using a common administrator account.
4. Finish the installation.
5. Repeat steps 1-4 to install any other systems you want to connect. They must all be installed using a common administrator account.

This approach cannot be used when **upgrading** workgroup installations, see Alternative upgrade for workgroup (on page 25).

Installation troubleshooting

The following issues may occur during or upon installation of the management server or recording servers. For each issue, one or more solutions are available.

Issue: Recording server startup fails due to port conflict

This issue can only appear if the Simple Mail Transfer Protocol (SMTP) service is running as it uses port 25. If port 25 is already in use for , it may not be possible to start the Recording Server service. It is important that port number 25 is available for the recording server's SMTP service.

SMTP Service: Verification and solutions

To verify whether SMTP Service is installed:

1. From Windows' *Start* menu, select *Control Panel*.
2. In the *Control Panel*, double-click *Add or Remove Programs*.
3. In the left side of the *Add or Remove Programs* window, click *Add/Remove Windows Components*.
4. In the *Windows Components* wizard, select *Internet Information Services (IIS)*, and click *Details*.
5. In the *Internet Information Services (IIS)* window, verify whether the *SMTP Service* check box is selected. If so, SMTP Service is installed.

If SMTP Service is installed, select one of the following solutions:

Solution 1: Disable SMTP Service, or set it to manual startup

This solution lets you start the recording server without having to stop the SMTP Service every time:

1. From Windows' *Start* menu, select *Control Panel*.
2. In the *Control Panel*, double-click *Administrative Tools*.
3. In the *Administrative Tools* window, double-click *Services*.
4. In the *Services* window, double-click *Simple Mail Transfer Protocol (SMTP)*.
5. In the *SMTP Properties* window, click *Stop*, then set *Startup type* to either *Manual* or *Disabled*.

When set to *Manual*, the SMTP Service can be started manually from the *Services* window, or from a command prompt using the command `net start SMTPSVC`.

6. Click *OK*.

Solution 2: Remove SMTP service

Removing the SMTP Service may affect other applications using the SMTP Service.

1. From Windows' *Start* menu, select *Control Panel*.
2. In the *Control Panel*, double-click *Add or Remove Programs*.
3. In the left side of the *Add or Remove Programs* window, click *Add/Remove Windows Components*.
4. In the *Windows Components* wizard, select the *Internet Information Services (IIS)* item, and click ***Details***.
5. In the *Internet Information Services (IIS)* window, clear the *SMTP Service* check box.
6. Click *OK*, *Next*, and *Finish*.

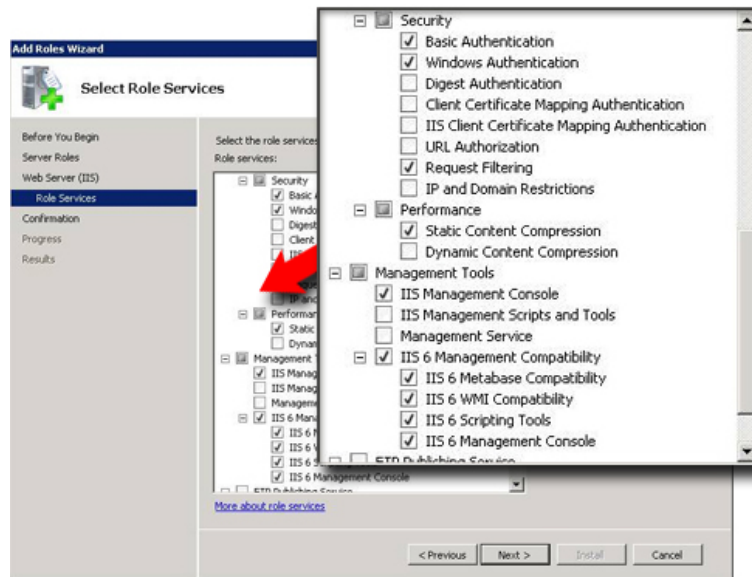
Issue: Automatic installation of IIS failed

The Internet Information Services (IIS) is normally installed automatically. If the automatic installation fails, you must install the IIS manually:

1. If automatic IIS installation fails, you see an error message asking you to install the IIS manually. In the error message box, click *Install IIS Manually*.

2. Select *Server Manager* from Windows' *Start* menu. In the left side of the *Server Manager* window, select *Roles*, then the *Roles Summary*.
3. Now select *Add Roles* to start a wizard.
4. In the wizard, click *Next*, select *Web Server (IIS)*, and follow the wizard's steps.
5. When you reach the wizard's **Select Role Services** step, you see that some role services are selected by default. However you should select some additional role services:
 - Under *Security*, select *Basic Authentication* and *Windows authentication*.
 - Under *Management Tools*, select *IIS Management Console*, expand it, and select *IIS 6 Metabase Compatibility*, *IIS 6 WMI Compatibility*, *IIS 6 Scripting Tools*, and *IIS 6 Management Console*.

When ready, the relevant part of the *Role services* tree should look like this:



6. Complete the wizard by following the remaining steps.

Issue: Changes to SQL server location prevents database access

This is an issue if the location of the SQL Server is changed, for example by changing the host name of the computer running the SQL Server. The result of this issue is that the access to the database is lost.

Solution: Use the update SQL address tool found at the tray icon, aka Systray.

Configure the system in Management Client

Here are the tasks typically involved in setting up an RC-L or RC-E system.

Even if information is presented as a checklist, a completed checklist does not in itself guarantee that the system matches the exact requirements of your organization. To make the system match the needs of your organization, OnSSI recommends that you monitor and adjust the system continuously.

For example, it is a good idea to test and adjust the motion detection sensitivity settings of individual cameras under different physical conditions (day/night, windy calm weather, and so on) once the system is running. The setup of rules, which determines most of the actions performed by the system (including when to record video), is another example of configuration which to a large extent depends on your organization's needs.

- ☒ You have finished the initial installation of your system.
See Install the system (on page 17).

- ☒ Change the trial SLC to a permanent SLC (if required).
See Change Software License Code (on page 23).
- ☒ Log in to the Management Client.
- ☐ Authorize use of your system's recording servers.
See Authorize a recording server (on page 33).
- ☐ Verify that each recording server's storage settings meet your needs.
See About storage and archiving (on page 36).
- ☐ Verify that each recording server's archiving settings meets your needs.
See Archive settings properties (on page 38).
- ☐ Detect the hardware (cameras or video encoders) to add to each recording server.
See Add hardware (on page 45).
- ☐ Configure each recording server's individual cameras.
See About camera devices (on page 54).
- ☐ Enable storage and archiving for individual cameras or a group of cameras. This is done from the individual cameras or from the device group.
See Attach a device or group of devices to a storage (on page 39).
- ☐ Enable and configure devices.
See Working with devices (on page 54).
- ☐ The behavior of the system is to a large extent determined by rules, such as when cameras should record, when PTZ (pan-tilt-zoom) cameras should patrol, when notifications should be sent.
Create rules.
See About rules and events (on page 81).
- ☐ Add roles to the system.
See About roles (on page 104).
- ☐ Add users and/or groups of users to each of the roles.
See Assign/remove users and groups to/from roles (on page 105).
- ☐ Activate licenses.
See Activate licenses (online) (see "Activate licenses online" on page 31) or Activate licenses (offline) (see "Activate licenses offline" on page 31).

Change Software License Code

If you run your installation on a trial Software License Code (SLC) during the first period, you can change it into a permanent SLC without any un- or reinstallation actions.

Important: This must be done locally on the management server. You **cannot** do this from the Management Client.

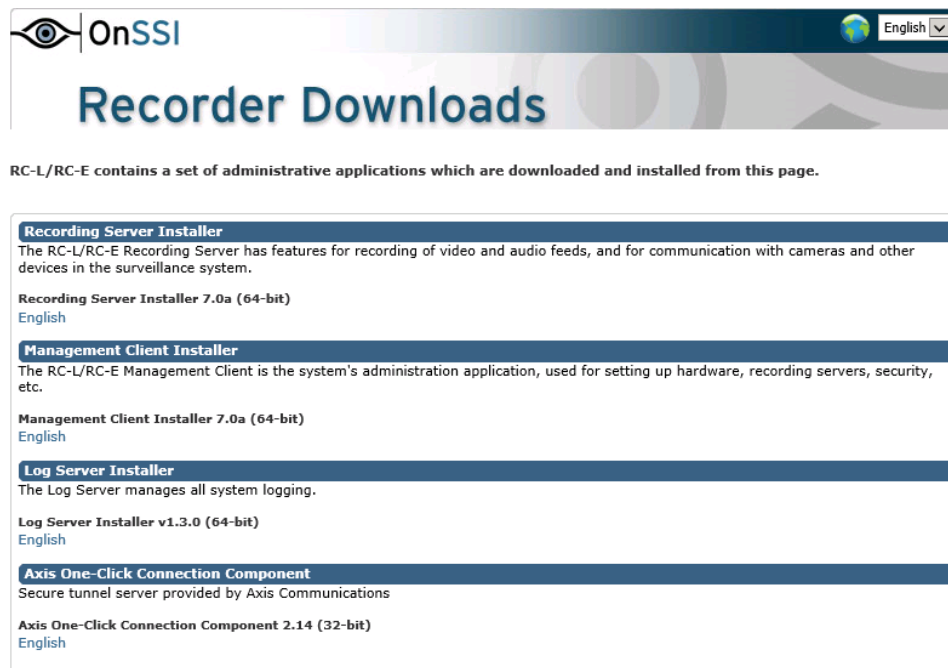
1. On the management server, go to the notification area of the taskbar.



2. Right-click the *Management Server* icon and select *Change License*.
3. Click *Import License*.
4. Next, select the SLC license file saved for this purpose. When done, the selected license file location is added just below the **Import License** button.
5. Click *OK* and you are now ready to register SLC. See Register Software License Code.

Recorder downloads web page

The management server includes a web page that enables administrators and end users to download and install required system components from any location, locally or remotely.



- The web page is targeted at **administrators**, enabling them to download and install key system components. Most often the web page is automatically loaded at the end of the management server installation and the default content is displayed.
- Access by entering the URL:

http://[management server address]:[port]/installation/admin/

where [management server address] is the IP address or host name of the management server, and [port] is the port number which you have configured IIS to use on the management server. If not accessing the web page on the management server itself, log in with an account which has administrator rights on the management server.

On the management server, you can access the webpage from Windows' *Start* menu, select *All Programs*, *OnSSI*, *Recorders*, *RC-L (or RC-E)*, *Administrative Installation Page*.

Upgrade

About upgrades

This information is only relevant if you are upgrading a previous installation.

Important: Neither RC-L nor RC-E support Microsoft Windows XP.

When you upgrade, all components, except the management server database, are automatically removed and replaced. This includes the drivers of your device pack.

The management server database contains the entire system configuration (recording server configurations, camera configurations, rules, and so on). As long as you do not remove the management server database, no reconfiguration of your system configuration is needed, even if you may want to configure some of the new features in the new version.

Backward compatibility with recording servers from versions older than this current version is limited. You can still access recordings on such older recording servers, but to be able to change their configuration, they must be of the same version as this current one. Therefore, it is highly recommended to upgrade all recording servers in your system.

When you do an upgrade including your recording servers, you are asked whether you want to **update** or **keep** your video device drivers. If you choose to update, it might take a few minutes for your hardware devices to make contact with the new video device drivers after restarting your system. This is due to several internal checks being performed on the newly installed drivers.

Upgrade prerequisites

- Have your **temporary license (.lic) file** ready. The license file changes when your SLC changes, so you may have received a new license file when you purchased the new version. When you install the management server, the wizard asks you to specify the location of your license (.lic) file, which the system verifies before you can continue.

If you do not have your license file, contact your Ocularis product vendor.

- Have your **new product version** ready.
- The management server stores your system's configuration in a database. The system configuration database can be stored in two different ways:
 1. In a SQL Server Express Edition database on the management server itself
 2. In a database on an existing SQL Server on your network.

If using 2), you must have **Administrator rights on the SQL Server** whenever you want to create, move or upgrade the management server's system configuration database on the SQL Server. Once you are done creating, moving or updating, being the database owner of the management server's system configuration database on the SQL Server is sufficient.

When you are ready to start the upgrade, follow the procedures in *Install the system* (on page 17).

Alternative upgrade for workgroup

If you do not use a domain setup, but a workgroup setup, you must do the following when you upgrade:

1. On the recording server, create a local Windows user.
2. From the Windows **Control Panel**, find the **RC-L_RC-E Data Collector service**. Right-click it, select **Properties**, and select the **Log on** tab. Set the Data Collector service to run as the local windows user you just created on the recording server.
3. On the management server, create the same local Windows user (with the same user name and password).
4. In the Management Client, add this local Windows user to the **Administrator's** group.

For installing with workgroups, see *Installation for workgroups* (on page 20).

First time use

Best practices

Protect recording databases from corruption

You can select which action to take if a camera database becomes corrupted. The actions include several database repair options. While it is good to have such options, OnSSI recommends that you take steps to ensure that your camera databases do not become corrupted.

Hard disk failure: protect your drives

Hard disk drives are mechanical devices and are vulnerable to external factors. The following are examples of external factors which may damage hard disk drives and lead to corrupt camera databases:

- Vibration (make sure the surveillance system server and its surroundings are stable)
- Strong heat (make sure the server has adequate ventilation)
- Strong magnetic fields (avoid)
- Power outages (make sure you use an Uninterruptible Power Supply (UPS))
- Static electricity (make sure you ground yourself if you are going to handle a hard disk drive).
- Fire, water, etc. (avoid)

Windows Task Manager: be careful when you end processes

When you work in Windows Task Manager, be careful not to end any processes which affect the surveillance system. If you end an application or system service by clicking *End Process* in the Windows Task Manager, the process is not be given the chance to save its state or data before it is terminated. This may lead to corrupt camera databases.

Windows Task Manager typically displays a warning if you attempt to end a process. Unless you are absolutely sure that ending the process is not going to affect the surveillance system, click *No* when the warning message asks you if you really want to terminate the process.

Power outages: use a UPS

The single-most common reason for corrupt databases is the recording server being shut down abruptly, without files being saved and without the operating system being closed down properly. This may happen due to power outages, due to somebody accidentally pulling out the server's power cable, or similar.

The best way of protecting your recording servers from being shut down abruptly is to equip each of your recording servers with a UPS (Uninterruptible Power Supply).

The UPS works as a battery-driven secondary power source, providing the necessary power for saving open files and safely powering down your system in the event of power irregularities. UPSs vary in sophistication, but many UPSs include software for automatically saving open files, for alerting system administrators, etc.

Selecting the right type of UPS for your organization's environment is an individual process. When you assess your needs, however, bear in mind the amount of runtime you require the UPS to be able to provide if the power fails. Saving open files and shutting down an operating system properly may take several minutes.

About daylight saving time

Daylight saving time (DST) is the practice of advancing clocks in order for evenings to have more daylight and mornings to have less. The use of DST varies between countries/regions.

When you work with a surveillance system, which is inherently time-sensitive, it is important that you know how the system handles DST.

Spring: Switch from Standard Time to DST

The change from standard time to DST is not much of an issue since you jump one hour forward. Typically, the clock jumps forward from 02:00 standard time to 03:00 DST, and the day has 23 hours. In that case, there is no data between 02:00 and 03:00 in the morning since that hour, for that day, did not exist.

Fall: Switch from DST to Standard Time

When you switch from DST to standard time in the fall, you jump one hour back. Typically, the clock jumps backward from 02:00 DST to 01:00 standard time, repeating that hour, and the day has 25 hours. In that case, you reach 01:59:59, then immediately revert back to 01:00:00. If the system did not react, it would essentially re-record that hour, so the first instance of, for example, 01:30 would be overwritten by the second instance of 01:30.

Because of this, your system forcefully archives the current video in the event that the system time changes by more than five minutes. The first instance of the 01:00 hour is not viewable directly from clients.

About time servers

Once your system receives images, they are instantly time-stamped. Since cameras are separate units which may have separate timing devices, camera time and your system time may not correspond fully. This may occasionally lead to confusion. If your cameras support timestamps, OnSSI recommends that you auto-synchronize camera and system time through a time server for consistent synchronization.

For information about how to configure a time server, search www.microsoft.com for *time server*, *time service*, or similar.

Management Client overview

About login authorization

If you encounter a second dialog during login, you need additional login authorization to get access to the Management Client.

When you log into the Management Client, you may be asked to for additional authorization of your login. You need a person who has the rights to authorize you to enter their credentials in the authorization login window.

If you do not know who can authorize you, ask your system administrator.

Management Client window

The Management Client window is divided into panes. The number of panes and layout depend on your:

- system configuration
- task
- available functions

Panes overview

Site Navigation pane: This is your main navigation element in the Management Client on the left. It reflects the name, settings and configurations of the site that you have logged in to. The site name is visible at the top of the pane. The features are grouped into categories that reflect the functionality of the software.

Federated Site Hierarchy pane: This is your navigation element that displays OnSSI Federated Architecture sites and their parent/child links.

The parent server that you are logged in to, your home site, is always at the top. If you adopt its point of view, you can view all its linked children and downwards in the parent/child hierarchy.

Overview Pane: Provides an overview of the element you have selected in the **Site Navigation** pane, for example a detailed list. When you select an element in the **Overview** pane, it typically displays the properties in the **Properties** pane. When you right-click elements in the **Overview** pane you get access to the management features.

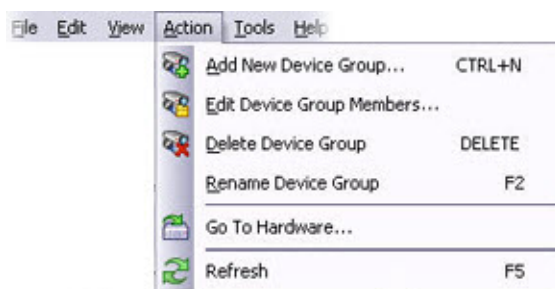
Properties pane: Displays properties of the element selected in the **Overview** pane. Often, properties are displayed across a number of tabs.

Preview pane: The **Preview** pane appears when you work with recording servers and devices. It shows preview images from the selected cameras or displays information about the state of the device.

By default, the information shown with the camera preview images concerns live streams. This is displayed in green text above the preview. If you want recording stream information instead (red text), select **View > Show Recording Streams** in the menu.

Performance can be affected if the **Preview** pane displays preview images from many cameras at a high frame rate. To control the number of preview images, and their frame rate, select **Options > General** in the menu.

Menu overview



Example only - some menus change depending on context.

File menu

You can save changes to the configuration and exit the application. You can also back up your configuration, see About backing up system configuration (see "About backing up and restoring your system configuration" on page 154).

Edit menu

You can undo changes.

View menu

Name	Description
Reset Application Layout	Reset the layout of the different panes in the Management Client to their default settings.
Preview Window	Toggle the Preview pane on and off when working with recording servers and devices.
Show Recording Streams	By default, the information shown with preview images in the Preview pane concerns live streams of the cameras. If you want information about recording streams instead, select <i>Show Recording Streams</i> .
Federated Site Hierarchy	By default, the Federated Site Hierarchy pane is enabled.
Site Navigation	By default, the Site Navigation pane is enabled.

Action menu

The content of the **Action** menu differs depending on the element you have selected in the **Site Navigation** pane. The actions you can choose from are the same as when you right-click the element. The elements are described in Management Client elements (on page 30).

Name	Description
Refresh	Is always available and reloads the requested information from the management server.

Tools menu

Name	Description
Registered Services	Manage registered services. See About the service channel (on page 164).
OnSSI Compatible Recording Servers	Add Ocularis CS servers to your system and manage the integration of the added servers. You can also use the feature to migrate from an Ocularis CS system to Ocularis ES. This is described in a separate document. <hr/> Only supported if your system: - runs Ocularis ES - uses IPv4 - works with RC-C/NetDVMS servers running version 6.0 and up
Effective Roles	View all roles of a selected user or group. <hr/> Only relevant if you run Ocularis ES.
Options	Opens the Options dialog box, which lets you define and edit global system settings. <hr/> Only relevant if you run Ocularis ES.

Help menu

You can access the help system and information about the version of the Management Client.

Management Client elements

Basics

License information

You can keep track of the licenses on this site and on all other sites licensed on the same software license code (SLC).

Installed Products

Lists all installed products on this site:

- Product version.
- Software license code (SLC).
- Expiry date of your SLC. Typically unlimited.

License Information

- Unlicensed hardware devices do not send data to the surveillance system, so the hardware device's cameras cannot be used for monitoring and recording.
- Hardware devices that you add after all available licenses are used, are listed as missing so they cannot be used for monitoring and recording.
- Devices connected to unlicensed hardware devices are identified by an exclamation mark in the Management Client. Note that the exclamation mark is used for other purposes.

Total - All Sites lists the status of licenses on all sites obtained with this SLC:

- License type - hardware device:
 - The total number of obtained and activated hardware device licenses on all sites using this SLC.
 - If you run Interconnect, the total number of obtained and activated Interconnect camera licenses on all sites using this SLC.

Current Site:

- The number of licenses on the current site:
 - The number of activated licenses and temporary (not activated) licenses.
 - If you need additional licenses for new hardware devices, add the number of missing licenses to the number of expired licenses to get the total number of required licenses.
- Expiry date of the next hardware device license appears in red below the table (if applicable). The date is counted from the day you added the hardware device.
- Drop-down list box to activate licenses online or offline.
- Button to access a license overview for all sites licensed via this SLC.

Devices which require a license

You need licenses for the number of hardware devices, for example video encoders or cameras, that you want to run on the system. One hardware device license enables you to run as many camera, speaker, microphone, input, output and metadata devices that the hardware device consists of. It also enables you to run the hardware device multiple times on one site or multiple times on multiple sites.

You need a camera license for each enabled interconnected camera in an Interconnect setup.

You can always get more licenses as your surveillance system grows, see [Get additional licenses](#) (on page 32).

View license overview

You can access a license overview that lists activated, temporary, expired and missing licenses for all sites licensed via this SLC.

- Click **License Overview**.

If the site is not a federated site or the connection is down, you can only view the number of activated licenses. N/A appears for temporary, expired, and missing licenses.

Activate licenses online

Activate your licenses online if the computer that runs the Management Client has Internet access.

1. On the **License Information** node, select **Activate License** and then **Active License Online**.
2. The *Activate Online* dialog box opens.
 - If you are an existing user, enter your user name and password to log into the software registration system.
 - If you are a new user, click the **Create new user** link to set up a new user account and then follow the registration procedure. If you have not yet registered your Software License Code (SLC), you must do so.
3. If you select *Save password*, the password is saved on the computer.
4. Click *Next* and follow the wizard's remaining steps to activate your licenses. Use the exact same user name under which you registered the SLC.
5. When you have activated your licenses, you see a confirmation.
6. Click *Finish* to end the activation.

If you receive an error message during online activation, follow the instructions on the screen to solve the issue.

If you have followed the instructions and still cannot access online activation, contact OnSSI Support, who investigates the issue for you.

Please also refer to the document *Ocularis Camera Licensing* for more information.

Activate licenses offline

If the computer that runs the Management Client does not have Internet access, you can activate licenses offline. First you export the license request and provide it to OnSSI, who then activates the licenses. When you receive the activated licenses, you import them into your system:

1. To export a file with your currently added cameras, click **Activate License**, and select **Activate License Offline > Export License For Activation**.
2. Specify a file name and a location for the license request (.lrq) file.
3. Send this .lrq file to support@onssi.com as an attachment.
4. An email is sent to you with an updated license file (.lic).
5. When you have received the updated license file (.lic), save it to a location accessible from the Management Client.
6. In the Management Client, click **License Information**.
7. Click **Activate License Offline > Import Activated License**, and select the .lic file to import it.
8. Click **Finish** to end the activation process.

Please also refer to the document *Ocularis Camera Licensing* for more information.

Activate licenses after grace period

If you do not activate an expired license within the grace period, the device becomes unavailable and cannot be used in the surveillance system.

- Configuration, added cameras, and other settings are not removed from the Management Client.
- The license is not deleted from the system configuration, so to enable the unavailable devices again, activate the license online or offline as usual.

Get additional licenses

If you want to add or if you have already added more hardware devices than you currently have licenses for, you must buy additional licenses to enable the devices to send data to your system.

1. To get additional licenses for your system, contact your product reseller.
2. When you have received an updated license file (.lic) with the new licenses, you must activate your licenses.

Licenses and hardware device replacement

You can replace a hardware device, such as camera, licensed in your system with a new device, and have the new device activated and licensed instead.

If you remove a hardware device from a recording server, you free up a license.

If you, for example, replace a camera with a similar camera (manufacturer, brand, and model), and give the new camera the same IP address, you maintain full access to all the camera's databases. In this case, you move the network cable from the old camera to the new one without changing any settings in the Management Client, and then activate the license.

If you replace a hardware device with a different model, you must use the *Replace Hardware* wizard (see Replace hardware (on page 160)) to map all relevant databases of cameras, microphones, inputs, outputs, and settings. When done, remember to activate the license.

Over time, there is a limit to the number of hardware devices you can replace depending on the number of hardware devices in your system. You receive a message from the system to contact Support, when you try to active a license online that exceeds the maximum number of allowed replacements.

Site information

You can add additional information to a site for an easier identification of each site, for example, in a large OnSSI Federated Architecture setup. Apart from the site name, you can describe:

- Address/location
- Administrator(s)
- Additional information

Update site information

To update site information:

1. Select **Edit**.
2. Select a tag.
3. Enter information in the **Value** field.
4. Click **OK**.

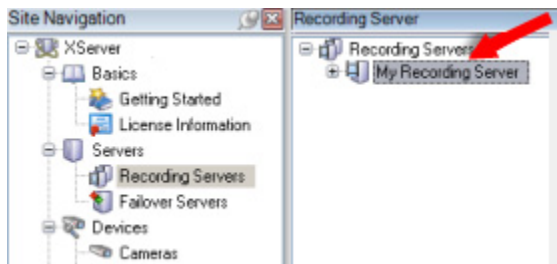
Servers and hardware

Recording servers

About recording servers

You use recording servers for recording video feeds, and for communicating with cameras and other devices. A surveillance system typically contains several recording servers, even though you only need a single recording server for the system to work.

Recording servers on your system, that is computers with the recording server software installed, and configured to communicate with a management server, are listed in the **Overview** pane when you expand the **Servers** folder and then select **Recording Servers**.



Recording server listed in Overview pane

Backward compatibility with recording servers from product versions older than this current version is limited. You can still access recordings on such older recording servers, but if you want to change their configuration, make sure they match the current version. OnSSI recommends that you upgrade all recording servers in your system to the same version as your management server.

Important: When the **Recording Server service** is running, it is very important that Windows Explorer or other programs do not access Media Database files or folders associated with your system setup. If they do, the recording server might not be able to rename or move relevant media files, which might bring the recording server to a halt. If this situation has already occurred, stop the Recording Server service, close the program accessing the relevant media file(s) or folder(s), and restart the Recording Server service.

Authorize a recording server

When you first use the system, or when you have added new recording servers to the system, you must authorize the new recording servers.

When you authorize a recording server, you configure it to connect to your management server.

1. Right-click the required recording server in the **Overview** pane.
2. Select **Authorize Recording Server**.



3. After a moment, the recording server is authorized and ready for further configuration via the tabs.

Change/verify the basic configuration of a recording server

If your Management Client does not list all the recording servers you have installed, the most likely reason is that you have configured the setup parameters (for example, the IP address or host name of the management server) incorrectly during installation.






You do not need to re-install recording servers to specify the parameters of the management servers, but you can change/verify its basic configuration:

1. On the computer that runs the recording server, right-click the **Recording Server** icon in the notification area.
2. Select *Stop Recording Server service*.
3. Right-click the *Recording Server* icon again and select *Change Settings*.
The *Recording Server Settings* window appears.
4. Verify/change the following settings:
 - **Management server hostname/IP address:** Specify the IP address or host name of the management server to which the recording server should be connected.
 - **Management server port:** Specify the port number to be used when communicating with the management server. Default is port 9993. You can change this if required, but the port number must always match the port number set up on the management server.
5. Click OK.
6. To start the Recording Server service again, right-click the *Recording Server* icon, and select *Start Recording Server service*.

Important: Stopping the Recording Server service means that you cannot record and view live video while you verify/change the recording server's basic configuration.

Recording server status icons

The Management Client uses the following icons to indicate the state of individual recording servers:

Icon	Description
	<i>Recording server is running</i>
	<i>Recording server is communicating</i>
	<p>Recording server requires attention: This icon typically appears because the Recording Server service is stopped.</p> <ol style="list-style-type: none"> 1) Right-click the recording server icon in the notification area. 2) Start/stop the Recording Server service and view recording server status messages.
	<p>Recording server must be authorized: Appears when you load the recording server for the first time. When you first use a recording server, you must authorize it:</p> <ol style="list-style-type: none"> 1) Right-click the required recording server icon. 2) Select <i>Authorize Recording Server</i>. After a moment, the recording server is authorized and ready for further configuration.
	<p>Ongoing database repair: Appears when databases are corrupted, for example due to a power failure, and the recording server is repairing them. The repair process may take some time if the databases are large.</p> <p>See Protect recording databases from corruption (on page 26) for information about how to avoid corrupt databases.</p> <hr/> <p>Important: During a database repair at startup, you cannot record video from cameras connected to the</p>

Icon	Description
	recording server. Only live viewing is available. <u>A database repair at normal operation does not affect any recordings.</u>

Info tab (recording server)

You can verify or edit the name and description of a selected recording server on the *Info* tab.



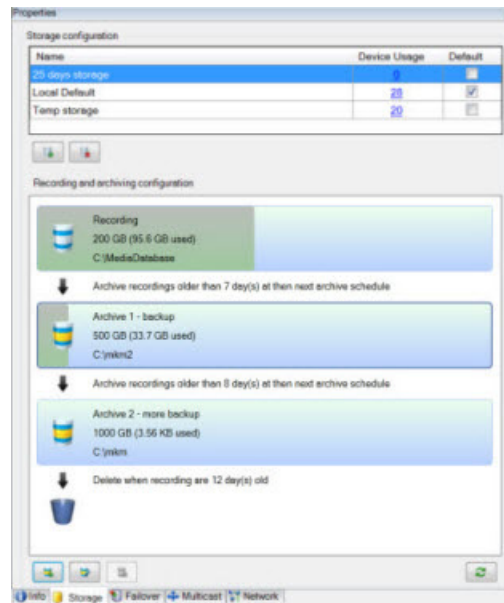
Info tab, displaying information about a recording server.

INFO TAB PROPERTIES

Name	Description
Name	Used when the recording server is listed in the system and clients. The name does not have to be unique. When you rename a recording server, the name is changed globally in the Management Client.
Description	The description appears in a number of listings within the system. A description is not mandatory.
Host name	Displays the recording server's host name.
Web server URL	Displays the URL of the recording server's web server. You use the web server, for example, for handling PTZ camera control commands, and for handling browse and live requests from Ocularis Client. The URL includes the port number used for web server communication (typically port 7563).
Time zone	Displays the time zone in which the recording server is located.

Storage tab (recording server)

On the *Storage* tab, you can setup, manage and view storages for selected recording servers.



ABOUT STORAGE AND ARCHIVING

When a camera records video or audio, all specified recordings are per default stored in the storage defined for the device, in the default recording database named *Recording*. A storage has no default archive(s), but you can create these.

To avoid that the recording database runs full, you can create additional storages. You can also create archives within each storage and start an archiving process to store data.

Archiving is the automatic transfer of recordings from, for example, a camera's default database to another location. In this way, the amount of recordings that you can store is not limited to the size of the recording database. With archiving you can also back up your recordings to another media.

You configure storage and archiving on a per-recording server basis.

As long as you store archived recordings locally or on accessible network drives, you can use Ocularis Client to view them with. This is also how you view recordings stored in a cameras' regular databases.

The following mostly mentions cameras and video, but speakers, microphones, audio and sound also apply.

Important: OnSSI recommends that you use a dedicated hard disk drive for the recording server database to prevent low disk performance. When you format the hard disk, it is important to change its *Allocation unit size* setting from 4 to 64 kilobytes. This is to significantly improve recording performance of the hard disk. You can read more about allocating unit sizes and find help at <http://support.microsoft.com/kb/140365/en-us>.

Important: The oldest data in a database is always auto-archived (or deleted if no next archive is defined) when less than 5GB of space is free. If less than 1GB space is free, data is deleted. A database always requires 250MB of free space. If you reach this limit because data is not deleted fast enough, no more data is written to the database until you free up enough space. The actual maximum size of your database becomes the amount of gigabytes that you specify, minus 5GB.

Attaching devices to a recording server

Once you have configured the storage and archiving settings for a recording server, you can enable storage and archiving for individual cameras or a group of cameras. This is done from the individual devices or from the device group. See *Attach a device or group of devices to a storage* (on page 39).

Effective archiving

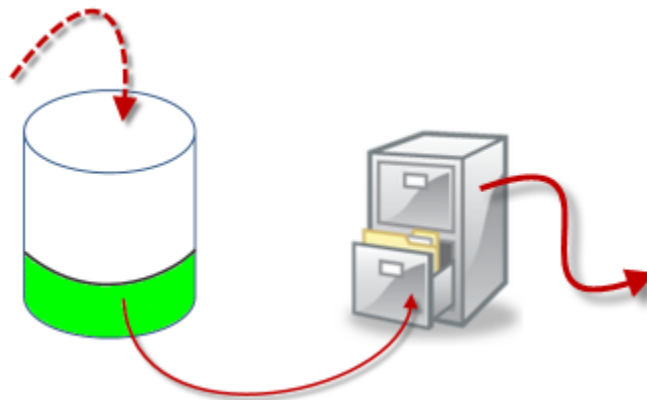
When you enable archiving for a camera or a group of cameras, the content of the camera database is automatically moved to an archive at intervals that you define.

Depending on your requirements, you can configure one or more archives for each of your databases. Archives can be located either on the recording server computer itself, or at another location which can be reached by the system, for example on a network drive.

By setting up your archiving in an effective way, you can prune and groom your database storage usage if needed. Often, you want to make archived recordings take up as little space as possible especially on a long-term basis, where it is perhaps even possible to slacken image quality a bit. You can handle effective pruning and grooming from the *Storage* tab of a recording server by adjusting several interdependent settings:

- Recording database retention
- Recording database size
- Archive retention
- Archive size
- Archive schedule
- Encryption
- Frames Per Second (FPS).

The size fields define the size of the camera's database, exemplified by the cylinder, and its archive(s) respectively:



Recordings' way from recording database to archive to deletion

By means of retention time and size setting for the recording database, exemplified by the white area in the cylinder, you define how old recordings must be before they are archived. In our illustrated example, you archive the recordings when they are old enough to be archived.

The retention time and size setting for archives define how long the recordings remain in the archive. Recordings remain in the archive for the time specified, or until the archive has reached the specified size limit. When these settings are met, the system begins to overwrite old recordings in the archive.

The archiving schedule defines how often and at what times archiving takes place.

FPS determines the size of the data in the databases.


To archive your recordings, you must set all these parameters up in accordance with each other. This means that the retention period of a next coming archive must always be longer than the retention period of a current archive or recording database. This is because the number of retention days stated for an archive includes all retention stated earlier in the process. Archiving must also always take place more frequently than the retention period, otherwise you risk losing data. If you have a retention time of 24 hours, any data older than 24 hours is deleted. Therefore, to get your data safely moved to the next archive, it is important to run archiving more often than every 24 hours.

Example: These storages (image to the left) have a retention time of 4 days and the following archive (image to the right) a retention time of 10 days. Archiving is set to occur every day at 10:30, ensuring a much more frequent archiving than retention time.

You can also control archiving by use of rules and events.

ADD A NEW STORAGE


You always create one storage with a predefined recording database named *Recording*. You cannot rename it. Apart from a recording database, a storage can contain a number of archives.

1. To add an extra storage to a selected recording server, click the  button located below the *Storage configuration* list. This opens the *Storage and Recording Settings* dialog box.
2. Specify the relevant settings to continue.
3. Click OK.

If needed, you are now ready to create archive(s) within your new storage. See *Create an archive within a storage* (on page 38).

CREATE AN ARCHIVE WITHIN A STORAGE

A storage has no default archive when it is created.

1. To create an archive, select the relevant storage in the *Recording and archiving configuration* list.
2. Click the  button below the *Recording and archiving configuration* list.
3. In the *Archive Settings* dialog box, specify the required settings (see *Archive settings properties* (on page 38)).
4. Click OK.

ARCHIVE SETTINGS PROPERTIES

In the **Archive** settings, specify the following:

Name	Description
<i>Name</i>	Rename the storage if needed. Names must be unique.
<i>Path</i>	Specify the path to the directory to which you save recordings in this storage. The storage does not necessarily have to be located on the recording server computer. If the directory does not exist, you can create it. Network drives must be specified by using UNC (Universal Naming Convention) format, example: \\server\volume\directory\.
<i>Retention time</i>	Specify for how long recordings should stay in the archive before they are deleted or moved to the next archive (depending on archive settings). The retention time must always be longer than the retention time of the previous archive or the default recording database. This is because the number of retention days specified for an archive includes all the retention periods stated earlier in the process.

Name	Description
<i>Maximum size</i>	<p>Select the maximum number of gigabytes of recording data to save in the recording database.</p> <p>Recording data in excess of the specified number of gigabytes is auto-moved to the first archive in the list - if any is specified - or deleted.</p> <p>Important: When less than 5GB of space is free, the system always auto-archives (or deletes if no next archive is defined) the oldest data in a database. If less than 1GB space is free, data is deleted. A database always requires 250MB of free space. If you reach this limit (if data is not deleted fast enough), no more data is written to the database until you have freed enough space. The actual maximum size of your database is the amount of gigabytes you specify, minus 5GB.</p>
<i>Schedule</i>	<p>Specify an archiving schedule that outlines the intervals with which the archiving process should start. You can archive very frequently (in principle every hour all year round), or very infrequently (for example, every first Monday of every 36 months).</p>
<i>Reduce frame rate</i>	<p>To reduce FPS when archiving, select the Reduce frame rate check box and set a frame per second (FPS).</p> <p>Reduction of frame rates by a selected number of FPS makes your recordings take up less space in the archive, but it also reduces the quality of your archive.</p> <p>MPEG/H.264 reduces automatically to key-frames as a minimum.</p> <p>0.1 = 1 frame per 10 seconds.</p>


ATTACH A DEVICE OR GROUP OF DEVICES TO A STORAGE

Once a storage area is configured for a recording server, you can enable it for individual devices such as cameras, microphones or speakers or a group of devices. You can also select which of a recording server's storage areas you want to use for the individual device or the group.

1. Expand *Devices* and select either *Cameras*, *Microphones* or *Speakers* as required.
2. Select the device or a device group.
3. Select the *Record* tab.
4. In the *Storage* area, select *Select*.
5. In the dialog box that appears, select the database that should store the recordings of the device and then click *OK*.
6. In the toolbar, click *Save*.

When you click the device usage number for the storage area on the *Storage* tab of the recording server, the device is visible in the message report that appears.

EDIT SETTINGS FOR A SELECTED STORAGE OR ARCHIVE

1. To edit a storage, select its recording database in the *Recording and archiving configuration* list. To edit an archive, select the archive database.
2. Click the  button located below the *Recording and archiving configuration* list.
3. Either edit a recording database or edit an archive.

If you change the maximum size of a database, the system auto-archives recordings that exceed the new limit. It auto-archives the recordings to the next archive or deletes them depending on archiving settings.

BACK UP ARCHIVED RECORDINGS

Many organizations want to back up their recordings by using tape drives or similar. Exactly how you do this is highly individual and depends on the backup media used in your organization. However, the following is worth bearing in mind:

Back up archives rather than camera databases

Always create backups based on the content of archives, not based on individual camera databases. If you create backups based on the content of individual camera databases you may cause sharing violations or other malfunctions.

When scheduling a backup, make sure the backup job does not overlap with your specified archiving times. To view each recording server's archiving schedule in each of a recording server's storage areas, see the Storage tab.

Know your archive structure so that you can target backups

When you archive recordings, you store them in a certain sub-directory structure within the archive.

During all regular use of your system, the sub-directory structure is completely transparent to the system's users when they browse all recordings with the Ocularis Client. This is true both with archived and non-archived recordings. It is relevant to know the sub-directory structure if you want to back up your archived recordings. See About archive structure (on page 40) and Backing up and restoring configuration (on page 154).

ABOUT ARCHIVE STRUCTURE

When you archive recordings, they are stored in a certain sub-directory structure within the archive.

During all regular use of your system, the sub-directory structure is completely transparent to the system's users, as they browse all recordings with the Ocularis Client regardless of whether the recordings are archived or not. Knowing the sub-directory structure is primarily interesting if you want to back up your archived recordings.

In each of the recording server's archive directories, the system automatically creates separate sub-directories. These sub-directories are named after the name of the device and the archive database.

Because you can store recordings from different cameras in the same archive, and since archiving for each camera is likely to be performed at regular intervals, further sub-directories are also automatically added.

These sub-directories each represent approximately an hour's worth of recordings. The one-hour split makes it possible to remove only relatively small parts of an archive's data if you reach the maximum allowed size of the archive.

The sub-directories are named after the device, followed by an indication of where the recordings came from (edge camera or via SMTP), *plus* the date and time of the most recent database record contained in the sub-directory.

Naming structure:

```
...[Storage Path]\[Storage name]\[device-name] - plus date and time of most recent recording\
```

If from edge camera:

```
...[Storage Path]\[Storage name]\[device-name] (Edge) - plus date and time of most recent recording\
```

If from SMTP:

```
...[Storage Path]\[Storage name]\[device-name] (SMTP) - plus date and time of most recent recording\
```

Real life example:

```
...F:\OurArchive\Archive1\Camera 1 on Axis Q7404 Video Server(10.100.50.137) - 2011-10-05T11:23:47+02:00\
```

Even further sub-directories are automatically added. The amount and nature of these sub-directories depend on the nature of the actual recordings. For example, several different sub-directories are added if the recordings are technically divided into sequences. This is often the case if you have used motion detection to trigger recordings.

If you want to back up your archives, you can target your backups if you know the basics of the sub-directory structure.

Examples of backup:

To back up the content of an entire archive, back up the required archive directory and all of its content. For example everything under:

```
...F:\OurArchive\
```


To back up the recordings from a particular camera from a particular period of time, back up the contents of the relevant sub-directories only. For example everything under:

```
...F:\OurArchive\Archive1\Camera 1 on Axis Q7404 Video Server(10.100.50.137) -  
2011-10-05T11:23:47+02:00\
```

DELETE AN ARCHIVE FROM A STORAGE AREA

1. Select the archive from the *Recording and archiving configuration* list.

It is only possible to delete the last archive in the list. The archive does not have to be empty.


2. Click the  button located below the *Recording and archiving configuration* list.
3. Click Yes.


DELETE AN ENTIRE STORAGE AREA

The storage area that you want to delete must **not** be set as default storage area and it must **not** be used by any devices to hold recordings.

This means that you may need to move devices and any not yet archived recordings that they have to another storage area before you delete the storage area.

1. To see the list of devices that use this storage area, click the device usage number.
2. Follow Move non-archived recordings from one storage to another (on page 41).
3. Continue until you have moved all devices.
4. Select the storage area that you want to delete.

Name	Device Usage	Default
25 days storage	9	
Local Default	28	<input checked="" type="checkbox"/>

5. Click the  button located below the *Storage configuration* list.
6. Click Yes.

MOVE NON-ARCHIVED RECORDINGS FROM ONE STORAGE TO ANOTHER

You move contents from one recording database to another from the *Record* tab of the device.

1. Select the device type. In the **Overview** pane, select the device.
2. Click the *Record* tab. In the upper part of the *Storage* area, click *Select*.
3. In the *Select Storage* dialog box, select the database.
4. Click OK.
5. In the *Recordings Action* dialog box, select whether already existing - but **non-archived** -recordings should be moved along to the new storage or deleted.
6. Click OK.

Failover tab (recording server)

Available functionality depends on the recorder you are using. See Differentiate LS and ES Recorders (on page 13) for more information.

If your organization uses failover recording servers, use the *Failover* tab to assign failover servers to recording servers, see Failover tab properties (on page 42).

For details on failover recording servers, installation and settings, failover groups and their settings, see About failover recording servers (regular and hot standby) (see "About failover recording servers" on page 131).

FAILOVER TAB PROPERTIES

Name	Description
<i>None</i>	Select a setup without failover.
<i>Primary failover server group / Secondary failover sever group</i>	Select a regular failover setup with one primary and possibly one secondary failover server group. Also, from the attached dropdown, select a primary failover group and possibly a secondary failover group.
<i>Hot standby server</i>	Select a hot standby setup. Also, from the dropdown, select a hot standby server.
<i>Advanced failover settings</i>	<p>Opens the Advanced Failover Settings window.</p> <ul style="list-style-type: none"> ▶ Full Support: Select to get full failover support for the device. ▶ Live Only: Select to get live failover support for the device. ▶ Disabled: Select to disable failover support for the device.
<i>Failover service communication port (TCP)</i>	By default, the port number is 11000. You use this port for communication between recording servers and failover recording servers. If you change the port, the recording server must be running and must be connected to the management server.

Multicast tab (recording server)

Your system supports multicasting of live streams from recording servers. If multiple Ocularis Client users want to view live video from the same camera, multicasting helps saving considerable system resources. Multicasting is particularly useful if you use the rare case where you use NetMatrix functionality, where multiple clients require live video from the same camera.

Multicasting is only possible for live streams, not for recorded video/audio.

If a recording server has more than one network interface card, it is only possible to use multicast on one of them. Through the Management Client you can specify which one to use.

The successful implementation of multicasting also requires that you have set up your network equipment to relay multicast data packets to the required group of recipients only. If not, multicasting may not be different from broadcasting, which can significantly slow down network communication.

ABOUT MULTICASTING

In regular network communication, each data packet is sent from a single sender to a single recipient - a process known as unicasting. But with multicasting you can send a single data packet (from a server) to multiple recipients (clients) within a group. Multicasting can help save bandwidth.

- When you use **unicasting**, the source must transmit one data stream for each recipient.
- When you use **multicasting**, only a single data stream is required on each network segment.

Multicasting as described here is **not** streaming of video from camera to servers, but from servers to clients.

With multicasting, you work with a defined group of recipients, based on options such as IP address ranges, the ability to enable/disable multicast for individual cameras, the ability to define largest acceptable data packet size (MTU), the maximum number of routers a data packet must be forwarded between (TTL), and so on.

Multicasting should not be confused with *broadcasting*, which sends data to everyone connected to the network, even if the data is perhaps not relevant for everyone:

Name	Description
Unicasting	Sends data from a single source to a single recipient.
Multicasting	Sends data from a single source to multiple recipients within a clearly defined group.
Broadcasting	Sends data from a single source to everyone on a network. Broadcasting can therefore significantly slow down network communication.

ENABLE MULTICASTING

To use multicasting, your network infrastructure must support the IP multicasting standard IGMP (Internet Group Management Protocol).

- On the *Multicast* tab, select the *Multicast* check box.

If the entire IP address range for multicast is already in use on one or more recording servers, you first release some multicast IP addresses before you can enable multicasting on additional recording servers.

ASSIGN IP ADDRESS RANGE

Specify the range you want to assign as addresses for multicast streams from the selected recording server. The clients connect to these addresses when the users view multicast video from the recording server.

For each multicast camera feed, the IP address and port combination must be unique (IPv4 example: 232.0.1.0:6000). You can either use one IP address and many ports, or many IP addresses and fewer ports. By default, the system suggests a single IP address and a range of 1000 ports, but you can change this as required.

IP addresses for multicasting must be within the range defined for dynamic host allocation by IANA. IANA is the authority overseeing global IP address allocation.

Name	Description
IP address	In the Start field, specify the first IP address in the required range. Then specify the last IP address in the range in the End field.
Port	In the Start field, specify the first port number in the required range. Then specify the last port number in the range in the End field.
Source IP address for all multicast streams	<p>You can only multicast on one network interface card, so this field is relevant if your recording server has more than one network interface card or if it has a network interface card with more than one IP address.</p> <p>To use the recording server's default interface, leave the value 0.0.0.0 (IPv4) or :: (IPv6) in the field. If you want to use another network interface card, or a different IP address on the same network interface card, specify the IP address of the required interface.</p> <ul style="list-style-type: none"> ▶ IPv4: 224.0.0.0 to 239.255.255.255.

SPECIFY DATAGRAM OPTIONS

Specify the settings for data packets (datagrams) transmitted through multicasting.

Name	Description
MTU	Maximum Transmission Unit, the largest allowed physical data packet size (measured in bytes). Messages larger than the specified MTU are split into smaller packets before they are sent. The default value is 1500, which is also the default on most Windows computers and Ethernet networks.
TTL	Time To Live, the largest allowed number of hops a data packet should be able to travel before it is discarded or returned. A hop is a point between two network devices, typically a router. Default value is 128.

ENABLE MULTICASTING FOR INDIVIDUAL CAMERAS

Multicasting only works when you enable it for the required cameras:

1. Select the recording server and select the required camera in the **Overview** pane.
2. On the **Client** tab, select the *Live multicast* check box. Repeat for all required cameras.

Network tab (recording server)

You define a recording server's public IP address on the *Network* tab.

WHY USE A PUBLIC ADDRESS?

When an access client, such as an Ocularis Client, connects to a surveillance system, an amount of initial data communication is shared in the background. This happens automatically, and is completely transparent to the users.

Clients may connect from the local network as well as from the Internet, and in both cases the surveillance system must provide suitable addresses so the clients can get access to live and recorded video from the recording servers:

- When clients connect locally, the surveillance system should reply with local addresses and port numbers.
- When clients connect from the Internet, the surveillance system should reply with the recording server's public address, that is the address of the firewall or NAT (Network Address Translation) router, and often also a different port number. The address and the port can then be forwarded to the server's local address and port.

To provide access to the surveillance system from outside a NAT (Network Address Translation) firewall, you can use public addresses and port forwarding. This allows clients from outside the firewall to connect to recording servers without using VPN (Virtual Private Network). Each recording server (and failover recording server) can be mapped to a specific port and the port can be forwarded through the firewall to the server's internal address.

DEFINE PUBLIC ADDRESS AND PORT

1. To enable public access, select the **Enable public access** check box.
2. Define the recording server's public address. Enter the address of the firewall or NAT router so clients that access the surveillance system from the Internet can connect to the recording servers.
3. Specify a public port number. It is always a good idea that port numbers used on the firewall or NAT router are different from the ones used locally.

If you use public access, configure the firewall or NAT router so requests sent to the public address and port are forwarded to the local address and port of relevant recording servers.

ASSIGN LOCAL IP RANGES

You define a list of local IP ranges which the surveillance system should recognize as coming from a local network.

- On the *Network* tab, click *Configure*.

Hardware and remote servers

About hardware

Hardware represents either:

- the physical unit that connects directly to the recording server of the surveillance system via IP, for example a camera, a video encoder, an I/O module or
- a recording server on a remote site:
 - Ocularis ES or
 - Ocularis LS or

See Add hardware (on page 45) to read about how to add hardware to your system.

Add hardware

You have several options for adding hardware for each recording server you have authorized on your system.

Important: If your hardware are located behind a NAT-enabled router or a firewall, you may need to specify a different port number and configure the router/firewall so it maps the port and IP addresses that the hardware uses.

The *Add Hardware* wizard helps you detect hardware like cameras and video encoders on your network and add them to the recording servers on your system. The wizard also helps you add remote recording servers for Interconnect setups. Only add hardware to **one recording server** at a time.

1. To access *Add Hardware*, right-click the required recording server and select *Add Hardware*.
2. Select one of the wizard options (see below) and follow the instruction on the screen.
3. After installation, you can see the hardware and it's devices in the **Overview** pane.

Name	Description
<i>Express</i> (Recommended)	<p>The system scans automatically for new hardware on the recording server's local network.</p> <p>Select the <i>Show hardware running on other recording servers</i> check box to see if detected hardware is running on other recording servers.</p> <p>You can select this option every time you add new hardware to your network and want to use it in your system.</p> <p>You cannot use this option to add remote systems in Interconnect setups.</p>
<i>Address range scanning</i>	<p>The system scans your network for relevant hardware and Interconnect remote systems based on your specifications of:</p> <ul style="list-style-type: none"> ▶ hardware user names and passwords. Not needed if your hardware use the factory default user names and passwords. ▶ drivers ▶ IP ranges (IPv4 only) ▶ port number (default = 80) <p>You can select this option when you only want to scan a part of your network, for example, when you expand your system.</p>
<i>Manual</i>	<p>Specify details about each hardware and Interconnect remote systems separately. This can be a good choice if you want to add only a few pieces of hardware, and you know their IP addresses, relevant user names and passwords or if a camera does not support the automatic discovery function.</p>

Name	Description
<i>Remote connect hardware</i>	<p>The system scans for hardware connected via a remotely connected server.</p> <p>You can use this option if you have installed servers for, for example, the Axis One-click Camera Connection.</p> <p>You cannot use this option to add remote systems in Interconnect setups.</p>

DISABLE/ENABLE HARDWARE

Added hardware is **enabled** by default.

You can see if hardware is enabled or disabled in this way:



Enabled



Disabled

To disable added hardware, for example, for licensing or performance purposes:

1. Expand the recording server, right-click the hardware you want to disable.
2. Select *Enabled* to clear or select it.

EDIT BASIC HARDWARE SETTINGS

You can edit basic settings, such as IP address/host name, for added hardware:

1. Expand recording server, right-click the hardware you want to edit.
2. Select *Edit Hardware*. This opens the *Edit Hardware* window, where you can edit relevant properties.
3. Click *OK*.

ENABLE/DISABLE INDIVIDUAL DEVICES

Cameras are **enabled** by default .

Microphones, speakers, metadata, inputs and outputs are **disabled** by default .

This means that microphones, speakers, metadata, inputs and outputs must be individually enabled before you can use them in the system. The reason for this is that surveillance systems rely on cameras, whereas the use of microphones and so on is highly individual depending on the needs of each organization.

You can see if devices are enabled or disabled (the examples show an output):



Disabled



Enabled

The same method for enabling/disabling is used for cameras, microphones, speakers, metadata, inputs, and outputs.

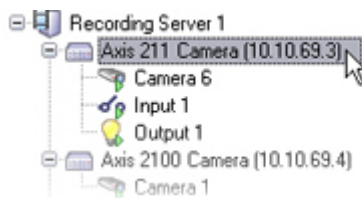
1. Expand the recording server and the device. Right-click the device you want to enable.
2. Select *Enabled* to clear or select it.

SET UP A SECURE CONNECTION TO THE HARDWARE

You can set up a secure HTTPS connection using SSL (Secure Sockets Layer) between the hardware and the recording server.

Consult your camera vendor to get a certificate for your hardware and upload it to the hardware, before you continue with the steps below:

1. In the **Overview** pane, right-click the recording server and select the hardware.



Selecting hardware under a recording server

2. On the *Settings* tab, enable HTTPS. This is not enabled by default.
3. Enter the port on the recording server to which the HTTPS connection is connected. The port number must correspond with the port set up on the device's homepage.
4. Make changes as needed and save.

Manage hardware

INFO TAB (HARDWARE)

For information about the **Info** tab for remote servers, see Info tab (remote server) (on page 49).

Info tab (hardware)

Name	Description
Name	Enter a name. The system uses the name whenever the hardware is listed in the system and in the clients. The name does not have to be unique. When you rename hardware, the name is changed globally in the Management Client.
Description	Enter a description of the hardware (optional). The description appears in a number of listings within the system. For example, when pausing the mouse pointer over the hardware name in the Overview pane: Example from a camera.
Model	Identifies the hardware model.
Version	Displays the firmware version of the system as specified by the manufacturer.
Serial number	Hardware serial number as specified by the manufacturer. The serial number is often, but not always, identical to the MAC address.
Driver	Identifies the driver that handles the connection to the hardware.
IE	Opens the default home page of the hardware vendor. You can use this page for administration of the hardware.
Address	The host name or IP address of the remote system.
MAC address	Specifies the Media Access Control (MAC) address of the system hardware. A MAC address is a 12-character hexadecimal number uniquely identifying each piece of hardware on a network.

SETTINGS TAB (HARDWARE)

On the **Settings** tab, you can verify or edit settings for the hardware.

The content of the **Settings** tab is determined by the selected hardware, and varies depending on the type of hardware. For some types of hardware, the **Settings** tab displays no content at all or read-only content.

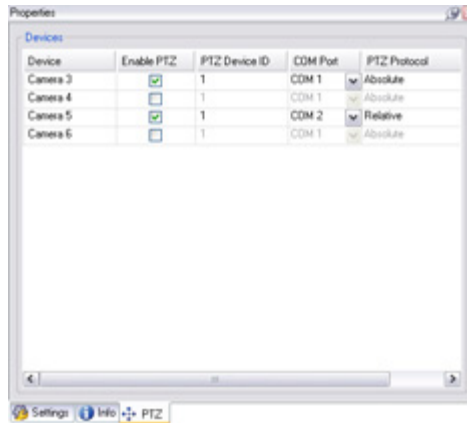
For information about the **Settings** tab for remote servers, see Settings tab (remote server) (on page 50).

PTZ TAB (VIDEO ENCODERS)

On the **PTZ** tab, you can enable PTZ (Pan/Tilt/Zoom) for video encoders. The tab is available if the selected device is a video encoder or if the driver supports both non-PTZ and PTZ cameras.

You must enable the use of PTZ separately for each of the video encoder's channels on the **PTZ** tab before you can use the PTZ features of the PTZ cameras attached to the video encoder.

Not all video encoders support the use of PTZ cameras. Even video encoders that support the use of PTZ cameras may require configuration before the PTZ cameras can be used. It is typically the installation of additional drivers through a browser-based configuration interface on the device's IP address.



PTZ tab, with PTZ enabled for two channels on a video encoder

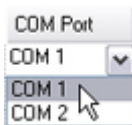
Enable PTZ on a video encoder

To enable the use of PTZ cameras on a video encoder, do the following on the *PTZ* tab:

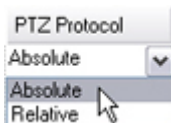
1. In the list of devices connected to the video encoder, select the *Enable PTZ* box for the relevant cameras:



2. In the *PTZ Device ID* column, verify the ID of each camera.
3. In the *COM Port* column, select which video encoder's COM (serial communications) ports to use for control of the PTZ functionality:



4. In the *PTZ Protocol* column, select which positioning scheme you want to use:



- **Absolute:** When operators use Pan/Tilt/Zoom controls for the camera, the camera is adjusted relative to a fixed position, often referred to as the camera's home position
- **Relative:** When operators use Pan/Tilt/Zoom controls for the camera, the camera is adjusted relative to its current position

The content of the **PTZ protocol** column varies a lot depending on the hardware. Some have 5 to 8 different protocols. See also the camera documentation.

5. In the toolbar, click *Save*.

You are ready to configure preset positions and patrolling for each PTZ camera:

- Add a preset position (type 1) (on page 65)
- Add a patrolling profile (on page 67)

Manage remote servers

INFO TAB (REMOTE SERVER)

Name	Description
Name	The system uses the name whenever the remote server is listed in the system and clients. The name does not have to be unique. When you rename a server, the name is changed globally in the Management Client.
Description	Enter a description of the remote server (optional). The description appears in a number of listings within the system. For example, when pausing the mouse pointer over the hardware name in the Overview pane.
Model	Displays the recorder name installed at the remote site.
Version	Displays the version of the remote system.
Software license code	The software license code of the remote system.
Driver	Identifies the driver that handles the connection to the remote server.
Address	The host name or IP address of the remote system.
IE	Opens the default home page of the hardware vendor. You can use this page for administration of the hardware or system.
Remote system ID	The unique system ID of the remote site used to, for example, manage licenses.
Windows user name	Enter the Windows user name for access through the remote desktop.
Windows password	Enter the Windows password for access through the remote desktop.
Connect	Opens a remote connection to the remote site (if Windows credentials are approved).

SETTINGS TAB (REMOTE SERVER)

On the **Settings** tab, you can view the name of the remote system.

EVENTS TAB (REMOTE SERVER)

You can add events from the remote system to your central site in order to create rules and thereby respond immediately to events from the remote system. The number of events depend on the events configured in the remote system. You cannot delete default events.

If the list appears to be incomplete:

1. Right-click the relevant remote server in the **Overview** pane and select **Update Hardware**.
2. The dialog box lists all changes (devices removed, updated and added) in the remote system since you established or last refreshed the Interconnect setup. Click **Confirm** to update your central site with these changes.

REMOTE RETRIEVAL TAB

On the **Remote Retrieval** tab, you can handle remote recording retrieval settings for the remote site in an Interconnect setup:

Specify the following properties:

Name	Description
Retrieve recordings at max	Determines the maximum bandwidth in Kbits/s to be used for retrieving recordings from a remote site. Select the check box to enable limiting retrievals.
Retrieve recordings between	<p>Determines that retrieval of recordings from a remote site are limited to a specific time interval.</p> <p>Unfinished jobs at the end time continue until completion, so if the end time is critical, you need to set it earlier to allow for unfinished jobs to complete.</p> <p>If the system receives an automatic retrieval or request for retrieval from the Ocularis Client outside the time interval, it is accepted, but not started until the selected time interval is reached.</p> <p>You can view pending remote recording retrieval jobs initiated by the users from System Dashboard -> Current Tasks.</p>
Retrieve on devices in parallel	Determines the maximum number of devices from which recordings are retrieved simultaneously. Change the default value if you need more or less capacity depending on your system's capabilities.

When you change the settings, it may take several minutes until the changes are reflected in the system.

None of the above applies to direct playback of remote recordings.

All cameras set to be played back directly is available for direct playback and use bandwidth as needed.

Remove a recording server

Important: If you remove a recording server, all configuration specified in the Management Client is removed for the recording server, including **all** of the recording server's associated hardware (cameras, input devices, and so on).

1. Right-click the recording server you want to remove in the **Overview** pane.
2. Select **Remove Recording Server**.
3. If you are sure, click **Yes**.
4. The recording server and all of its associated hardware are removed.

Delete all hardware on a recording server

Important: When you delete hardware, all recorded data related to the hardware is deleted permanently.

1. Right-click the recording server on which you want to delete all hardware.
2. Select **Delete All Hardware**.
3. Confirm the deletion.

Devices

The devices appear in the Management Client when you add hardware with the **Add Hardware** wizard.

You can manage devices via the device groups if they have the same properties, see About device groups (on page 52).

You can also manage the devices individually:

- Cameras
- Microphones
- Speakers
- Metadata
- Inputs
- Outputs

See About devices (on page 54).

Working with device groups

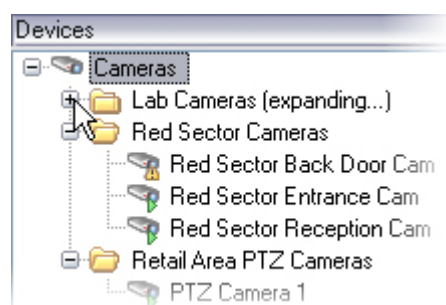
About device groups

Grouping of devices into device groups is part of the **Add Hardware** wizard, but you can always modify the groups and add more groups if needed.

You can benefit from grouping different types of devices (cameras, microphones, speakers, metadata, inputs, and outputs) on your system:

- Device groups help you maintain an intuitive overview of devices on your system.
- Devices can exist in several groups.
- You can create subgroups and subgroups in subgroups.
- You can specify common properties for all devices within a device group in one go.
- Device properties set via the group are not stored for the group but on the individual devices.
- When dealing with roles, you can specify common security settings for all devices within a device group in one go.
- When dealing with rules, you can apply a rule for all devices within a device group in one go.

You can add as many device groups as required, but you cannot mix different types of devices (for example cameras and speakers) in a device group.



Example: cameras grouped into device groups

Create device groups with **less** than 400 devices so you can view and edit all properties.

If you delete a device group, you only delete the device group itself. If you want to delete a device, for example a camera, from your system, do it on the recording server level.

The following examples are based on grouping cameras into device groups, but the principles apply for all devices:

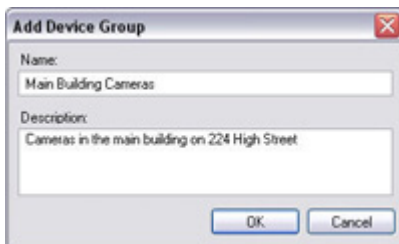
Add a device group (on page 53)

Specify which devices to include in a device group (on page 53)

Specify common properties for all devices in a device group (on page 54)

Add a device group

1. In the **Overview** pane, right-click the device type under which you want to create a device group.
2. Select *Add Device Group*.
3. In the *Add Device Group* dialog box, specify a name and description of the new device group:



The description appears when you pause the mouse pointer over the device group in the device group list.

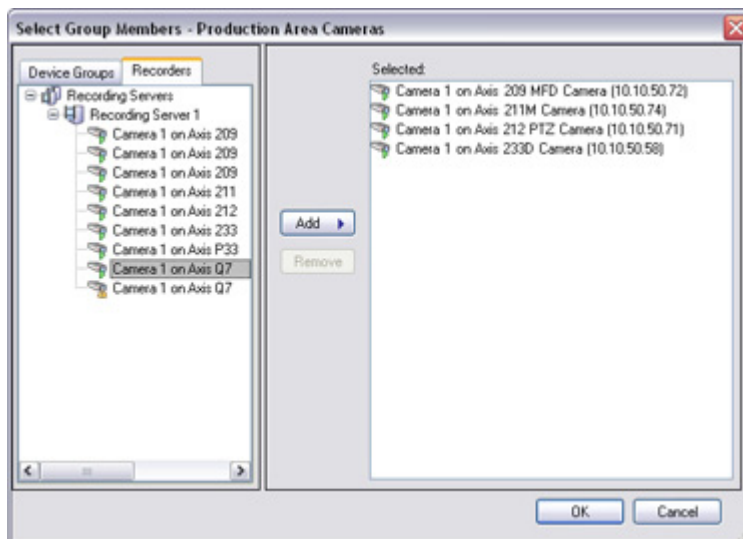
4. Click **OK**. A folder representing the new device group appears in the list.
5. Continue with *Specify which devices to include in a device group* (on page 53).

Specify which devices to include in a device group

1. In the **Overview** pane, right-click the relevant device group folder.
2. Select *Edit Device Group Members*.
3. In the *Select Group Members* window, select one of the tabs to locate the device.

A device can be a member of more than one device group.

4. Select the devices you want to include, and click *Add* or double-click the device:



5. Click **OK**.

- If you exceed the limit of 400 devices in one group, you can add device groups as subgroups under other device groups:



Specify common properties for all devices in a device group

With device groups, you can specify common properties for all devices within a given device group:

- In the **Overview** pane, click the device group.
In the **Properties** pane, all properties *which are available on all of the device group's devices* are listed and grouped on tabs.
- Specify the relevant common properties.
On the **Settings** tab, you can switch between settings for *all* devices and settings for individual devices.
- In the toolbar, click **Save**. The settings are saved on the individual devices, not in the device group.

Working with devices

About devices

Hardware has a number of devices that you can manage individually, for example:

- A physical camera has devices that represent the camera part (lenses) as well as microphones, speakers, metadata, input and output either attached or built-in.
- A video encoder has multiple analog cameras connected that appear in one list of devices that represent the camera part (lenses) as well as microphones, speakers, metadata, input and output either attached or built-in.
- An I/O module has devices that represent the input and output channels for, for example, lights.
- A dedicated audio module has devices that represent microphones and speaker inputs and outputs.
- In an Interconnect setup, the remote system appears as hardware with all devices from the remote system listed in one list.

The system automatically adds the hardware's devices when you add hardware.

The following sections describe each of the device types with links to the tabs you can use to manage them.

About camera devices

Camera devices are added automatically when you add hardware to the system and are by default enabled.

Camera devices deliver video streams to the system that the client users can use to view live video or that the system can record for later playback by the client users. Roles determine the users' right to view video.

The system comes with a default start feed rule which ensures that video feeds from all connected cameras are automatically fed to the system. Like other rules, the default rule can be deactivated and/or modified as required.

Enabling/disabling and renaming of individual devices take place on the recording server hardware. See [Enable/disable devices via device groups](#) (on page 58).

For all other configuration and management of cameras, expand **Devices** in the Site Navigation pane, then select **Cameras**. In the Overview pane, you group your cameras for an easy overview of your cameras. Initial grouping is done as part of the **Add hardware** wizard.

Follow this configuration order to complete the most typical tasks related to configuration of a camera device:

1. Configure camera settings (see Settings tab (see "Settings tab (devices)" on page 60)).
2. Configure streams (see Streams tab (see "Streams tab (devices)" on page 61)).
3. Configure motion (see Motion tab (see "Motion tab (devices)" on page 74)).
4. Configure recording (see Record tab (see "Record tab (devices)" on page 62)).
5. Configure the remaining settings as needed.

About microphone devices

On many devices you can attach external microphones. Some devices have built-in microphones.

Microphone devices are added automatically when you add hardware to the system. They are per default disabled, so you must enable them before use, either as part of the *Add Hardware* wizard or afterwards. Microphones do not require separate licenses. You can use as many microphones as required on your system.

You can use microphones completely independently of cameras.

Microphone devices deliver audio streams to the system that the client users can listen to live or the system can record for later playback by the client users. You can set up the system to receive microphone specific events that trigger relevant actions.

Roles determine the users' right to listen to microphones. You cannot listen to microphones from the Management Client.

The system comes with a default start audio feed rule which ensures that audio feeds from all connected microphones are automatically fed to the system. Like other rules, the default rule can be deactivated and/or modified as required.

Enabling/disabling and renaming of individual devices take place on the recording server hardware. See Enable/disable devices via device groups (on page 58).

For all other configuration and management of cameras, expand **Devices** in the Site Navigation pane, then select **Microphones**. In the Overview pane, you group your microphones for an easy overview. Initial grouping is done as part of the *Add hardware* wizard.

You can configure microphone devices on these tabs:

- Info tab (see "Info tab (devices)" on page 60)
- Settings tab (see "Settings tab (devices)" on page 60)
- Record tab (see "Record tab (devices)" on page 62)
- Events tab (see "Events tab (devices)" on page 69)

About speaker devices

On many devices you can attach external speakers. Some devices have built-in speakers.

Speaker devices are added automatically when you add hardware to the system. They are per default disabled, so you must enable them before use, either as part of the *Add Hardware* wizard or afterwards. Speakers do not require separate licenses. You can use as many speakers as required on your system.

You can use speakers completely independently of cameras.

The system sends an audio stream to the speakers when a user presses the talk button in Ocularis Client. Speaker audio is only recorded when talked to by an user. Roles determine users' right to talk through speakers. You cannot talk through speakers from the Management Client.

If two users want to speak at the same time, the roles determine users' right to talk through speakers. As part of the roles definition, you can specify a speaker priority from very high to very low. If two users want to speak at the same time, the user whose role has the highest priority wins the ability to speak. If two users with the same role want to speak at the same time, the first-come first-served principle applies.

The system comes with a default start audio feed rule that starts the device so the device is ready to send user activated audio to the speakers. Like other rules, the default rule can be deactivated and/or modified as required.

Enabling/disabling and renaming of individual devices take place on the recording server hardware. See Enable/disable devices via device groups (on page 58).

For all other configuration and management of cameras, expand **Devices** in the Site Navigation pane, then select **Speakers**. In the Overview pane, you group your speakers for an easy overview. Initial grouping is done as part of the **Add hardware** wizard.

You can configure speaker devices on these tabs:

- Info tab (see "Info tab (devices)" on page 60)
- Settings tab (see "Settings tab (devices)" on page 60)
- Record tab (see "Record tab (devices)" on page 62)

About metadata devices

Metadata devices deliver data streams to the system that the client users can use to view data about data, for example, data that describes the video image, the content or objects in the image, or the location of where the image was recorded. Metadata can be attached to cameras, microphones, or speakers.

Metadata can be generated by:

- The device itself delivering the data, for example the camera delivering video.
- A 3rd party system or integration via a generic metadata driver.

The device-generated metadata is automatically linked to one or more devices on the same hardware.

Roles determine the users' right to view metadata.

The system comes with a default start feed rule which ensures that metadata feeds from all connected hardware that supports metadata, are automatically fed to the system. Like other rules, the default rule can be deactivated and/or modified as required.

Enabling/disabling and renaming of individual devices take place on the recording server hardware. See Enable/disable devices via device groups (on page 58).

For all other configuration and management of metadata devices, expand **Devices** in the Site Navigation pane, then select **Metadata**. In the Overview pane, you group your metadata devices for an easy overview. Initial grouping is done as part of the **Add hardware** wizard.

You can configure metadata devices on these tabs:

- Info tab (see "Info tab (devices)" on page 60)
- Settings tab (see "Settings tab (devices)" on page 60)
- Record tab (see "Record tab (devices)" on page 62)

About input devices

On many devices you can attach external units to input ports on the device. Input units are typically external sensors. You can use such external sensors, for example, for detecting if doors, windows, or gates are opened. Input from such external input units is treated as events by the system.

You can use such events in rules. For example, you could create a rule specifying that a camera should begin recording when an input is activated, and stop recording 30 seconds after the input is deactivated.

You can use input devices completely independently of cameras.

Before you specify use of external input units on a device, verify that the device itself recognize the sensor operation. Most devices can show this in their configuration interfaces, or via Common Gateway Interface (CGI) script commands.

Input devices are added automatically when you add hardware to the system. They are per default disabled, so you must enable them before use, either as part of the **Add Hardware** wizard or afterwards. Input devices do not require separate licenses. You can use as many input devices as required on your system.

Enabling/disabling and renaming of individual devices take place on the recording server hardware. See Enable/disable devices via device groups (on page 58).

For all other configuration and management of cameras, expand **Devices** in the Site Navigation pane, then select **Input**. In the Overview pane, you group your input devices for an easy overview. Initial grouping is done as part of the **Add hardware** wizard.

You can configure input devices on these tabs:

- Info tab (see "Info tab (devices)" on page 60)
- Settings tab (see "Settings tab (devices)" on page 60)
- Events tab (see "Events tab (devices)" on page 69)

ACTIVATE INPUT MANUALLY FOR TEST

With the rules feature, you define rules that automatically activate or deactivate input or you can activate them manually and check the result in the Management Client:

1. In the **Overview** pane, select the relevant input device.
2. Activate the input on the physical device.
3. In the **Preview** pane, see if the indicator lights up green. Then the input device works.

About output devices

On many devices you can attach external units to output ports on the device. This allows you to activate/deactivate lights, sirens, etc. through the system.

You can use output when creating rules. You can create rules that automatically activate or deactivate outputs, and rules that trigger actions when the state of an output is changed.

Output can be triggered manually from the Management Client and Ocularis Client.

Before you specify use of external output units on a device, verify that the device itself can control the device attached to the output. Most devices can show this in their configuration interfaces, or via Common Gateway Interface (CGI) script commands.

Output devices are added automatically when you add hardware to the system. They are per default disabled, so you must enable them before use, either as part of the **Add Hardware** wizard or afterwards. Output devices do not require separate licenses. You can use as many output devices as required on your system.

Enabling/disabling and renaming of individual devices take place on the recording server hardware. See Enable/disable devices via device groups (on page 58).

For all other configuration and management of cameras, expand **Devices** in the Site Navigation pane, then select **Output**. In the Overview pane, you group your input devices for an easy overview. Initial grouping is done as part of the **Add hardware** wizard.

You can configure output devices on these tabs:

- Info tab (see "Info tab (devices)" on page 60)
- Settings tab (see "Settings tab (devices)" on page 60)


ACTIVATE OUTPUT MANUALLY FOR TEST

With the rules feature, you define rules that automatically activate or deactivate output or you can activate them manually from a client.


You can activate an output manually from the Management Client to test the functionality:

1. In the **Overview** pane, select the relevant output device.
2. Typically, the following elements are shown for each output in the **Preview** pane:



3. Select/clear the check box ☒  to activate/deactivate the selected output. When an output is activated, the indicator lights up green:



4. Alternatively, click the rectangular button  to activate the output for the duration defined in the *Output Trigger Time* setting on the *Settings* tab (this feature/setting may not be available for all outputs). After the defined duration, the output is automatically deactivated.

Enable/disable devices via device groups

You can enable/disable devices only via the configured hardware. Unless manually enabled/disabled in the add hardware wizard, camera devices are per default enabled and all other devices are per default disabled.

To locate a device via the device groups to enable or disable:

1. In the **Site Navigation** pane, select the device.
2. In the **Overview** pane expand the relevant group and find the device.
3. Right-click the device, and select *Go To Hardware*.
4. Click the plus node to see all devices on the hardware.
5. Right-click the device you want to enable/disable, and select *Enabled*.

Status icons of devices

When you select a device, information about the current status appears in the **Preview** pane.
The following icons indicate the status of the devices:

Cam- era	Micro- phone	Spea- ker	Meta- data	In- put	Out- put	Description
						Device enabled and retrieving data: The device is enabled and you retrieve a live stream.
						Device recording: The device is recording data on the system.
						Device temporarily stopped or has no feed: When stopped, no information is transferred to the system. If it is a camera, you cannot view live video. A stopped device can still communicate with the recording server for retrieving events, setting settings etc., as opposed to when a device is disabled.
						Devices disabled: Cannot be started automatically through a rule and cannot communicate with the recording server. If a camera is disabled, you cannot view live or recorded video.
						Device database being repaired.
						Device requires attention: The device does not function correctly. Pause the mouse pointer over the device icon to get a description of the problem in the tooltip.
						Status unknown: Status of the device is unknown, for example, if the recording server is offline.
						Note that some icons can be combined, as in this example where Device enabled and retrieving data is combined with Device recording .

Info tab (devices)

ABOUT THE INFO TAB

On the *Info* tab, you can view and edit basic information about a device in a number of fields. All devices have an *Info* tab.

INFO TAB PROPERTIES

Name	Description
Name	The name is used whenever the device is listed in the system and clients. When you rename a device, the name is changed globally in the Management Client.
Description	Enter a description of the device (optional). The description appears in a number of listings within the system. For example, when you pause the mouse pointer over the name in the Overview pane.
Hardware name	Displays the name of the hardware, with which the device is connected. The field is non-editable from here, but you can change it by clicking <i>Go To</i> next to it. This takes you to hardware information where you can change the name.
Port number	Displays the port on which the device is attached on the hardware. For single-device hardware, the port number is typically 1. For multi-device hardware, such as video servers with several channels, the port number typically indicates the channel on which the device is attached, for example 3.

Settings tab (devices)

ABOUT THE SETTINGS TAB

On the *Settings* tab, you can view and edit settings for a device in a number of fields. All devices have a *Settings* tab.

The values appear in a table as changeable or read-only. When you change a setting to a non-default value, the value appears **in bold**.

The content of the table depends on the device driver.

ABOUT CAMERA SETTINGS

You can view or edit settings, such as:

- default frame rate
- resolution
- compression
- the maximum number of frames between keyframes
- on-screen date/time/text display for a selected camera, or for all cameras within a device group.

The drivers for the cameras determine the content of the *Settings* tab. The drivers vary depending on the type of camera.

For cameras that support more than one type of stream, for example MPEG4, MJPEG, and H.264, you can use multi-streaming, see About multi-streaming (on page 61).

When you change a setting, you can quickly verify the effect of your change if you have the **Preview** pane enabled. You cannot use the **Preview** pane to judge the effect of frame rate changes because the **Preview** pane's thumbnail images use another frame rate defined in the **Options** dialog box.

If you change the settings for **Max. frames between keyframes** and **Max. frames between keyframes mode**, it may lower the performance of some functionalities in Ocularis Client. For example, Ocularis Client requires a keyframe to start up showing video, so a longer period between keyframes, may prolong the Ocularis Client start up.

Streams tab (devices)

ABOUT THE STREAMS TAB

The following devices have a *Streams* tab:

- Cameras

The *Streams* tab lists by default a single stream. It is the selected camera's default stream, used for live and recorded video.

For live streaming, you can set up and use as many live streams as the camera supports, but you can only select one stream for recording at a time. To change which stream to use for recording, select the *Record* box for the stream to be recorded.

ABOUT MULTI-STREAMING

Playback of recorded video and viewing live video do not necessarily require the same video quality and frame rate to achieve the best result. You can have **either** one stream for live viewing and another stream for playback purposes **or** multiple separate live streams with different resolution, encoding, and frame rate.

Example 1, live and recorded video:

- For viewing **live** video, your organization may prefer MPEG4 at a high frame rate.
- For playing back **recorded** video, your organization may prefer MJPEG at a lower frame rate because this preserves disk space.

Example 2, multiple live videos:

- For viewing **live video from a local operating point**, your organization may prefer MPEG4 at a high frame rate to have the highest quality of video available.
- For viewing **live video from a remotely connected operating point**, your organization may prefer MJPEG at a lower frame rate and quality in order to preserve network bandwidth.

Even when cameras support multi-streaming, individual multi-streaming capabilities may vary between different cameras. See the camera's documentation for more information.

To see if a camera offers different types of streams, see the *Settings* tab. The number of available streams in an Interconnect setup depends on the capabilities of the interconnected system.

ADD A STREAM

1. On the *Streams* tab, click *Add*. This adds a second stream to the list.
2. In the *Name* column, edit the name of the stream. The name appears in Ocularis Client.
3. In the *Live Mode* column, select when live streaming is needed.
 - **Always:** the stream runs even if no Ocularis Client users request the stream.
 - **Never:** the stream is off. Only use this for recording streams, for example, if you want recordings in high quality and need the bandwidth.
 - **When needed:** the stream starts when an Ocularis Client user requests for it.
4. In the *Default* column, select which stream is default.
5. In the *Record* column, select the check box if you want to record this stream or leave it cleared if you only want to use it for live video.

6. In the *Remote Recording* column, select the check box if you want to use this recording stream for retrieving remote- and edge recordings.
7. Click *Save*.

Record tab (devices)

ABOUT THE RECORD TAB

The following devices have a *Record* tab:

- Cameras
- Microphones
- Speakers
- Metadata

Recordings from a device are only saved in the database when you have enabled recording and the recording-related rule criteria are met.

Parameters that cannot be configured for a device are grayed out.

ENABLE PLAYBACK DIRECTLY FROM REMOTE SITE CAMERA

1. On the central site, expand **Servers** and select **Recording Servers**.
2. In the Overview pane, expand the required recording server, select the relevant remote system. Select the relevant camera.
3. In the Properties pane, select the **Record** tab, and select the **Play back recordings from remote system** option.
4. In the toolbar, click *Save*.

In an Interconnect setup, the central system disregards privacy masking defined in a remote system.

ENABLE/DISABLE RECORDING

Recording is by default enabled. To enable/disable recording:

1. Select the device.
2. Select/clear the *Record* tab's *Recording* check box.

You must enable recording for the device before you can record data from the camera. A rule that specifies the circumstances for a device to record does not work if you have disabled recording the device.

ENABLE RECORDING ON RELATED DEVICES

For camera devices, you can enable recording for related devices that are connected to the same recording server. It means that the related devices record when the camera records.

Recording on related devices are enabled by default for new camera devices, but you can disable and enable as you want. For existing camera devices in the system, the check box is cleared by default.

1. Select/clear the **Record on related devices** box.
2. On **Camera > Client** tab, specify the devices that relate to this camera.

If you want to enable recording on related devices that are connected to another recording server, you must create a rule.

ABOUT PRE-BUFFERING

Pre-buffering is the ability to record audio and video before the actual triggering event occurs. This is useful when you want to record the audio or video that leads up to an event that triggers recording, for example, opening a door.

Pre-buffering is possible because the system continuously receives audio and video streams from the connected devices and temporarily stores them in the media database for the defined pre-buffer period.

- If a recording rule is triggered, the temporary recordings are made permanent for the rule's configured pre-recording time.
- If no recording rule is triggered the temporary recordings in the pre-buffer are automatically deleted after the defined pre-buffer time.

To use the pre-buffer function, the devices must be enabled and sending a stream to the system.

Devices that support pre-buffering

Cameras, microphones and speakers support pre-buffering. For speakers, the streams are only sent when an Ocularis Client user uses the **Talk to speaker** function. This means that depending on how your speaker streams are triggered to be recorded there is little or no pre-buffering available.

In most cases you set up speakers to record when the Ocularis Client user uses the **Talk to speaker** function. In such cases, no speaker pre-buffer is available.

MANAGE PRE-BUFFERING

Enable and disable pre-buffering:

Pre-buffering is enabled by default with a pre-buffer size of three seconds.

1. To enable/disable pre-buffering, select/clear the *Pre-buffer (in seconds)* check box.
2. When you enable it, specify a pre-buffer size. The number of seconds you specify must be sufficiently large to accommodate your requirements in the various recording rules you define.

Use pre-buffer in rules:

When you create rules that trigger recording, you can select that recordings should start some time before the actual event (pre-buffer).

To use the pre-buffer recording function in the rule, you must enable pre-buffering on the device being recorded and you must set the pre-buffer length to at least the same length as specified in the rule.

MANAGE MANUAL RECORDING

Stop manual recording after is enabled by default with a recording time of five minutes. This is to ensure that the system automatically stops all recordings started by the Ocularis Client users.

☒ Stop manual recording after: minutes

1. To enable and disable manual recording to be stopped automatically by the system, select/clear the **Stop manual recording after** check box.
2. When you enable it, specify a recording time. The number of minutes you specify must be sufficiently large to accommodate the requirements of the various manual recordings without overloading the system.

Add to roles:

You must grant the right to start and stop manual recording to the client users on each camera in **Roles** on the **Device** tab.

Use in rules:


The events you can use when you create rules related to manual recording are:

- **Manual Recording Started**
- **Manual Recording Stopped**

SPECIFY RECORDING FRAME RATE

You can specify the recording frame rate for JPEG.

- Select or type the recording frame rate (in FPS, frames per second) in the **Recording frame rate: (JPEG)** box.



Specifying a specific recording frame rate

ENABLE KEYFRAME RECORDING

You can enable keyframe recording for H.264 and MPEG4 streams. It means that the system switches between recording keyframes only and recording all frames depending on your rule settings.

You can, for example, let the system record keyframes when there is no motion in the view and switch to all frames only in case of motion detection to save storage.

1. Select the **Record keyframes only** box.



Enabling keyframe recording

2. Set up a rule that activates the function, see About actions and stop actions (on page 82).

ABOUT STORAGE

Under **Storage**, you can monitor and edit database settings for the device.

At the top, you can see the selected database and its status.

Possible statuses for selected database:

Name	Description
Active	Database is active and running.
Archives also located in old storage	Database is active and running and has archives located in other storage areas as well.
Data for some of the devices chosen is currently moving to another location	Database is active and running and is moving data for one or more selected devices in a group from one location to another.
Data for the device is currently moving to another location	Database is active and running and is moving data for the selected device from one location to another.
Information unavailable in failover mode	Status information about the database cannot be collected when database is in failover mode.

For information about configuration of storage, see About storage and archiving (on page 36).

ABOUT REMOTE RECORDING

The remote recording option is only available if the selected camera supports edge storage or is a camera in an Interconnect setup.

To ensure that all recordings are saved in case of network issues, select ***Automatically retrieve remote recordings when connections are restored***. This enables automatic retrieval of recordings once connection is re-established.

The type of hardware selected determines where recordings are retrieved from:

- For a camera with local recording storage, recordings are retrieved from the camera's local recording storage.
- For an Interconnect remote system, recordings are retrieved from the remote systems' recording servers.

You can use the following functionality independently of the automatic retrieval:

- Manual recording.
- The ***Retrieve and store remote recordings from <devices>*** rule.
- The ***Retrieve and store remote recordings between <start and end time> from <devices>*** rule.

Presets tab (devices)

ABOUT THE PRESETS TAB

The following devices have a *Presets* tab:

- PTZ cameras that support preset positions

On the *Presets* tab, you can create or import preset positions, for example:

- In rules for making a PTZ (Pan/Tilt/Zoom) camera move to a specific preset position when an event occurs.
- In patrolling, for the automatic movement of a PTZ camera between a number of preset positions.
- For manual activation by the Ocularis Client users.

ADD A PRESET POSITION (TYPE 1)

To add a preset position for the camera:

1. Click *Add New*. The *Add Preset* window appears.
2. The *Add Preset* window displays a live preview image from the camera. Use the navigation buttons and/or sliders to move the camera to the required position.
3. Specify a name for the preset position in the *Name* field.
4. Optionally, type a description of the preset position in the *Description* field.
5. Click **Add** if you want to specify more presets.
6. Click *OK*. The *Add Preset* window closes, and adds the position to the *Presets* tab's list of available preset positions for the camera.

USE PRESET POSITIONS FROM THE CAMERA (TYPE 2)

As an alternative to specifying preset positions in the system, you can specify preset positions for some PTZ cameras on the camera itself. You can typically do this by accessing a product-specific configuration web page.

1. Import the presets into the system by selecting *Use presets from device*.

2. Any presets you have previously defined for the camera are deleted and affect any defined rules and patrolling schedules as well as remove the presets available for the Ocularis Client users.
3. If you later want to edit such device-defined presets, edit on the camera and then re-import.

ASSIGN A DEFAULT PRESET POSITION

If required, you can assign one of a PTZ camera's preset positions as the camera's default preset position.

It can be useful to have a default preset position because it allows you to define rules that specify that the PTZ camera should go to the default preset position under particular circumstances, for example after you have operated the PTZ camera manually.

1. To assign a preset position as the default, select the preset in your list of defined preset positions.
2. Select the *Default preset* check box below the list.

You can only define one preset position as the default preset position.

EDIT A PRESET POSITION (TYPE 1 ONLY)

To edit an existing preset position defined in the system:

1. Select the preset position in the *Presets* tab's list of available preset positions for the camera.
2. Click *Edit*. This opens the *Edit Preset* window:
3. The *Edit Preset* window displays a live preview image from the preset position. Use the navigation buttons and/or sliders to change the preset position as required.
4. Change the name/number and description of the preset position as required.
5. Click *OK*.

TEST A PRESET POSITION (TYPE 1 ONLY)

1. Select the preset position in the *Presets* tab's list of available preset positions for the camera.
2. Click **Activate**.
3. The camera moves to the selected preset position.

Patrolling tab (devices)

ABOUT THE PATROLLING TAB

The following devices have a *Patrolling* tab:

- Cameras

On the *Patrolling* tab, you can create patrolling profiles - the automatic movement of a PTZ (Pan/Tilt/Zoom) camera between a number of preset positions.

Before you can work with patrolling, you must specify at least two preset positions for the camera in the **Presets** tab.

Patrolling profiles are the definitions of how patrolling should take place. This includes the order in which the camera should move between preset positions and how long it should remain at each position. You can create an unlimited number of patrolling profiles and use them in your rules. For example, you may create a rule specifying that one patrolling profile should be used during daytime opening hours and another during nights.

ADD A PATROLLING PROFILE

Add a profile that you want to use in a rule:

1. Click *Add*. The *Add Profile* dialog box appears.
2. In the *Add Profile* dialog box, specify a name for the patrolling profile.
3. Click *OK*. The new patrolling profile is added to the *Profile* list. You can now specify the preset positions and other settings for the patrolling profile.

SPECIFY PRESET POSITIONS IN A PATROLLING PROFILE

1. Select the patrolling profile in the *Profile* list.
2. Click *Add*.
3. In the *Select Preset* dialog box, select the preset positions for your patrolling profile:
4. Click *OK*. The selected preset positions are added to the list of preset positions for the patrolling profile:
5. The camera uses the preset position at the top of the list as the first stop when it patrols according to the patrolling profile. The preset position in second position from the top is the second stop, and so forth.

SPECIFY THE TIME AT EACH PRESET POSITION

When patrolling, the PTZ camera by default remains for 5 seconds at each preset position specified in the patrolling profile.

To change the number of seconds:

1. Select the patrolling profile in the *Profile* list.
2. Select the preset position for which you want to change the time:



3. Specify the time in the *Wait time (sec.)* field:
4. If required, repeat for other preset positions.

CUSTOMIZE TRANSITIONS

By default, the time required for moving the camera from one preset position to another, known as *transition*, is estimated to be three seconds. During this time, motion detection is by default disabled on the camera, because irrelevant motion is otherwise likely to be detected while the camera moves between the preset positions.

You can only customize speed for transitions if your camera supports PTZ scanning and is of the type where preset positions are configured and stored on your system's server (type 1 PTZ camera). Otherwise the *Speed* slider is grayed out.

You can customize the following:

- The estimated transition time
- The speed with which the camera moves during a transition
- Which plug-ins to disable during transition.

To customize transitions between the different preset positions:

1. Select the patrolling profile in the *Profile* list.
2. Select the *Customize transitions* check box.

Transition indications are added to the list of preset positions.

3. In the list, select the transition.
4. Specify the estimated transition time (in number of seconds) in the *Expected time (sec.)* field.
5. Use the *Speed* slider to specify the transition speed. When the slider is in its rightmost position, the camera moves with its default speed. The more you move the slider to the left, the slower the camera moves during the selected transition.
6. In the *Plug-ins to disable* list, specify any plug-ins you want to disable during the selected transition. By default, the plug-in used for motion detection on the camera (*MotionDetectionPlugin*) is disabled in order to avoid irrelevant motion being detected during transition.
1. To add a plug-in that you want to disable during the transition, click *Add*, and select the plug-in.
2. To remove a plug-in from the list, for example if you want motion detection enabled during the transition, select the plug-in and click *Remove*.
7. Repeat as required for other transitions.

SPECIFY AN END POSITION

You can specify that the camera should move to a specific preset position when patrolling according to the selected patrolling profile ends.

1. Select the patrolling profile in the *Profile* list.
2. Select the *Go to specific preset on finish* check box. This opens the *Select Preset* dialog box.
3. In the *Select Preset* dialog box, select the end position, and click *OK*.

You can select any of the camera's preset positions as the end position, you are not limited to the preset positions used in the patrolling profile.

4. The selected end position is added to the profile list.

When patrolling according to the selected patrolling profile ends, the camera moves to the specified end position.

SPECIFY MANUAL PTZ SESSION TIMEOUT

Ocularis Client users can manually interrupt the patrolling of PTZ cameras.

You can specify how much time should pass before regular patrolling is resumed after a manual interruption:

1. Select *Tools > Options*.
2. On the *Options* window's *General* tab, select the amount of time in the *PTZ manual session timeout* list (default is 15 seconds).

The setting applies for all PTZ cameras on your system.

360° Lens tab (devices)

This tab is not used with Ocularis. Configuration is performed in *Ocularis Administrator*.

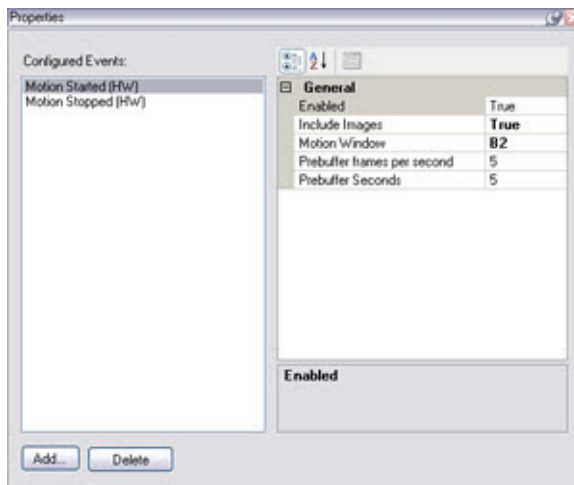
Events tab (devices)

ABOUT THE EVENTS TAB

The following devices have an *Events* tab:

- Cameras
- Microphones
- Inputs

In addition to the system's event, some devices can be configured to trigger events. You can use these events when creating event-based rules in the system. Technically, they occur on the actual hardware/device rather than on the surveillance system.



Event tab, example from camera

When you delete an event, it affects all rules that use the event.

- Add an event (on page 69)
- Specify event properties (on page 70)
- Use several instances of an event (on page 70)

ADD AN EVENT

1. In the **Overview** pane, select a device.
2. Select the *Events* tab and click *Add*. This opens the *Select Driver Event* window.
3. Select an event. You can only select one event at a time.
4. Click *OK*.
5. In the toolbar, click *Save*.

SPECIFY EVENT PROPERTIES

You can specify properties for each event you have added. The number of properties depends on the device and the event. In order for the event to work as intended, you must specify some or all of the properties identically on the device as well as on this tab.

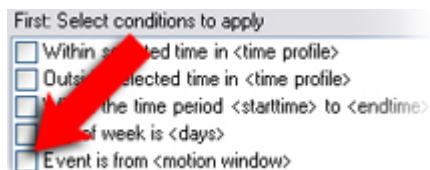
USE SEVERAL INSTANCES OF AN EVENT

To be able to specify different properties for different instances of an event, you can add an event more than once.

The following example is specific to **cameras**.

Example: You have configured the camera with two motion windows, called A1, and A2. You have added two instances of the *Motion Started (HW)* event. In the properties of one instance, you have specified the use of motion window A1. In the properties of the other instance, you have specified the use of motion window A2.

When you use the event in a rule, you can specify that the event should be based on motion detected in a specific motion window for the rule to be triggered:



Example: Specifying specific motion window as part of a rule's conditions

EVENT TAB (PROPERTIES)

Name	Description
Configured events	Which events you may select and add in the Configured events list is determined entirely by the device and its configuration. For some types of devices, the list is empty.
General	The list of properties depends on the device and the event. In order for the event to work as intended, you must specify some or all of the properties identically on the device as well as on this tab.

Client tab (devices)

ABOUT THE CLIENT TAB

The following devices have a *Client* tab:

- Cameras

On the *Client* tab you can specify which other devices are viewed and heard when you use the camera in Ocularis Client.

The related devices also record when the camera records, see Enable recording on related devices (on page 62).

CLIENT TAB PROPERTIES

Name	Description
<i>Live multicast</i>	<p>The system supports multicast of live streams from the recording server to Ocularis Client. To enable multicast of live streams from the selected camera, select the check box.</p> <p>You must also configure multicasting for the recording server. See About multicasting (on page 42).</p> <p>If multicast streams do not work, for example due to restrictions on the network or on individual clients, the system reverts to unicast.</p>
<i>Related microphone</i>	<p>Specify from which microphone on the camera, that Ocularis Client users by default receive audio. The Ocularis Client user can manually select to listen to another microphone if needed.</p> <p>The related microphones record when the camera records.</p>
<i>Related speaker</i>	<p>Specify through which speakers on the camera, that Ocularis Client users speak by default. The Ocularis Client user can manually select another speaker if needed.</p> <p>The related speakers record when the camera records.</p>
<i>Related metadata</i>	<p>Specify one or more metadata devices on the camera, that Ocularis Client users receive data from.</p> <p>The related metadata devices record when the camera records.</p>
<i>Shortcut</i>	This field is not used with Ocularis.

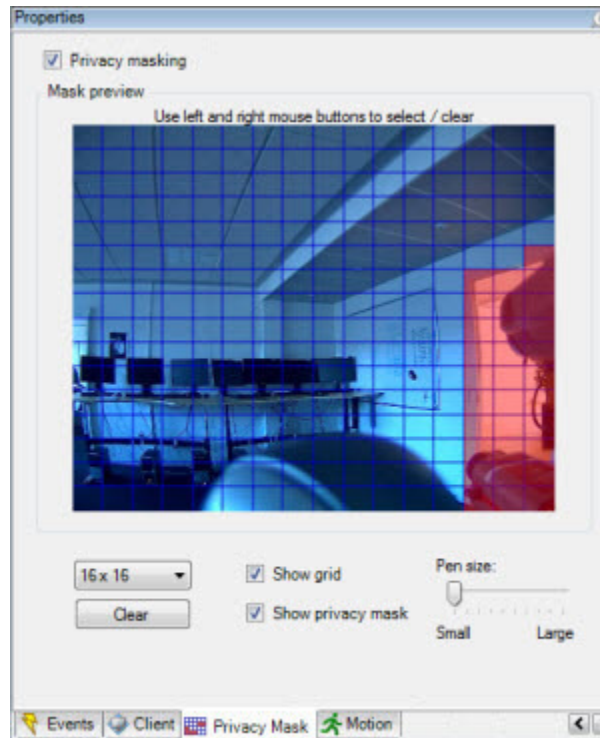
Privacy mask tab (devices)**ABOUT THE PRIVACY MASK TAB**

The following devices have a *Privacy Mask* tab:

- Cameras

On the *Privacy Mask* tab, you can enable and configure privacy masking for the selected camera. You can define which areas of the image to mask before distribution. For example, if a surveillance camera covers a street, in order to protect residents privacy, you can mask certain areas of a building (could be windows and doors) with privacy masking.

When viewed via Ocularis Client or any other media, privacy masked areas appear as black areas which no one can remove.



Red areas indicate the areas masked for privacy.

When you use privacy masks with PTZ cameras and you pan/tilt/zoom the camera, the selected area masked for privacy does **not** move accordingly because the masked area is locked to the camera image. As an alternative, some PTZ cameras support enabling of a position based privacy mask in the camera itself.

In an Interconnect setup, the central system disregards privacy masking defined in a remote system.

ENABLE/DISABLE PRIVACY MASKING

The privacy masking feature is disabled by default.

To enable/disable the privacy masking feature for a camera:

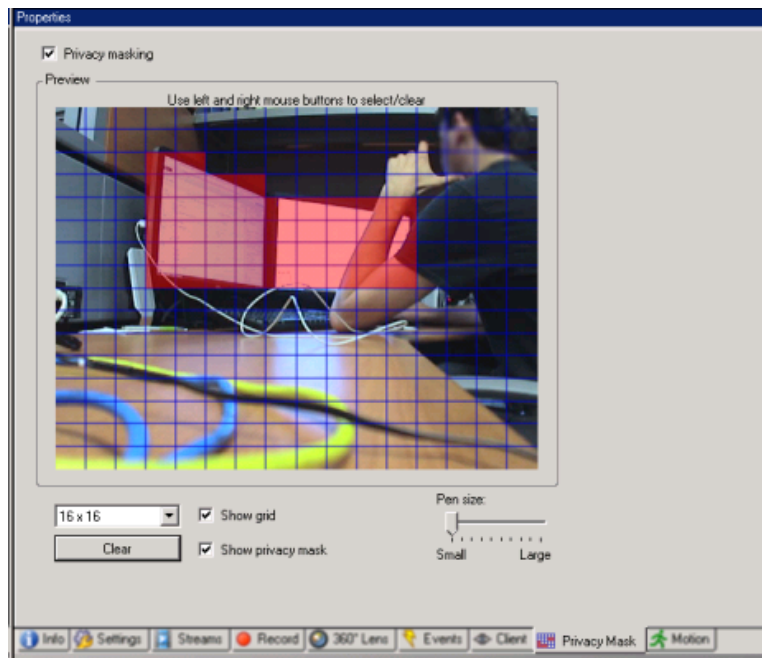
- Select/clear the *Privacy Mask* tab's *Privacy masking* check box.

SPECIFY PRIVACY MASK SETTINGS

When you enable privacy masking, the preview image is divided into selectable sections by a grid.

1. To define privacy mask regions, drag the mouse pointer over the required areas in the preview image. Press down the left mouse button to select a grid section. Right mouse button clears a grid section.

2. You can define as many privacy mask regions as needed. Privacy mask regions are shown in red.



Two privacy mask regions defined in the preview window. In this case, the grid is visible.

The red privacy mask indications also appears in the preview image on the *Motion* tab.

PRIVACY MASK TAB (PROPERTIES)

Name	Description
Grid Size	The value you selected in the <i>Grid size</i> list determines the density of the grid, regardless whether the grid is shown or not. Select between the values 8×8, 16×16, 32×32 or 64×64.
Show Grid	Select the <i>Show grid</i> check box to make the grid visible.
Show Privacy Mask	When you select the <i>Show privacy mask</i> check box (default), selected regions are highlighted in red in the preview image. Hiding regions may provide a less obscured view of the preview image. OnSSI recommends that you keep the <i>Show privacy mask</i> box selected to avoid that regions exist without you or your colleagues being aware of it.
Pen size	Use the <i>Pen size</i> slider to indicate the size of the selections you wish to make when you click and drag the grid to select regions. Default is set to small, which is equivalent to one square in the grid.

Motion tab (devices)

ABOUT THE MOTION TAB

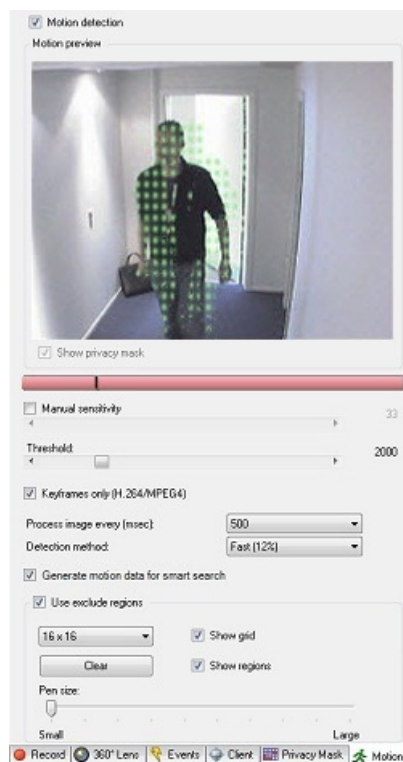
The following devices have a *Motion* tab:

- Cameras

On the *Motion* tab, you can enable and configure motion detection for the selected camera. Motion detection configuration is a key element in your system: Your motion detection configuration determines when the system generates motion events and typically also when video is recorded.

Time spent on finding the best possible motion detection configuration for each camera helps you later avoid, for example, unnecessary recordings. Depending on the physical location of the camera, it may be a good idea to test motion detection settings under different physical conditions such as day/night and windy/calm weather.

Before you configure motion detection for a camera, OnSSI recommends that you have configured the camera's image quality settings, for example resolution, video codec and stream settings on the *Settings* tab. If you later change image quality settings, you should always test any motion detection configuration afterwards.



Camera properties: *Motion* tab with red deflection on the motion indication bar

You can configure all the settings for a group of cameras, but you would typically set the exclude regions per camera.

- Enable and disable motion detection (on page 74)
- Specify motion detection settings (on page 75)

ENABLE AND DISABLE MOTION DETECTION

You specify the default setting of motion detection for cameras on the **Tools > Options > General** tab.

To enable or disable motion detection afterwards for a camera:

- Select or clear the **Motion** tab's **Motion detection** check box.

Important: When you disable motion detection for a camera, motion detection-related rules for the camera do not work.

SPECIFY MOTION DETECTION SETTINGS

You can specify settings related to the amount of changes required in a camera's view in order for the change to be regarded as motion. You can for example specify intervals between motion detection analysis and areas of a view in which motion should be ignored.

About dynamic sensitivity

Motion detection is per default set up for dynamic sensitivity. To adjust the sensitivity level manually, see Enable manual sensitivity (on page 75).

OnSSI recommends that you do not enable manual sensitivity because:

- With dynamic sensitivity, the system calculates and optimizes the sensitivity level automatically and suppresses the motion detections that come from noise in the images.
- Dynamic sensitivity improves motion detection at nighttime, where the noise in the images often triggers false motion.
- The system is not overloaded from too much recording.
- The users are not missing results from too little recording.

Enable manual sensitivity

The sensitivity setting determines **how much each pixel** in the image must change before it is regarded as motion.

1. Select the *Motion* tab's *Manual Sensitivity* check box.
2. Drag the slider to the left for a higher sensitivity level, and to the right for a lower sensitivity level.
The *higher* the sensitivity level, the less change is allowed in each pixel before it is regarded as motion.
The *lower* the sensitivity level, the more change in each pixel is allowed before it is regarded as motion.
Pixels in which motion is detected are highlighted in green in the preview image.
3. Select a slider position in which only detections you consider motion are highlighted.

You can compare and set the exact sensitivity setting between cameras by the number in the right side of the slider.

Specify threshold

The motion detection threshold determines **how many pixels** in the image must change before it is regarded as motion.

1. Drag the slider to the left for a higher motion level, and to the right for a lower motion level.
2. Select a slider position in which only detections that you consider motion are detected.

The black vertical line in the motion indication bar shows the motion detection threshold: When detected motion is above the selected detection threshold level, the bar changes color from green to red, indicating a positive detection.



Motion indication bar: changes color from green to red when above the threshold, indicating a positive motion detection

Select keyframes settings

Determines if motion detection is done on keyframes only instead of on the entire video stream. Only applies to MPEG4 and H.264.

Motion detection on keyframes reduces the amount of processing power used to carry out the analysis.

- Select **Keyframes only (MPEG)** to do motion detection on keyframes only.

Select image processing interval

You can select how often the system performs the motion detection analysis.

From the *Process image every (msec)* list:

- Select the interval. For example, every 1000 milliseconds is once every second. Default value is every 500 milliseconds.

The interval is applied if the actual frame rate is higher than the interval you set here.

Specify detection method

Lets you optimize motion detection performance by analyzing only a selected percentage of the image, for example 25%. By analyzing 25%, only every fourth pixel in the image is analyzed instead of all pixels.

Using optimized detection reduces the amount of processing power used to carry out the analysis, but also means a less accurate motion detection.

- In the *Detection method* drop down-box, select the wanted detection method.

About generate motion data for smart search

With **Generate motion data for smart search** enabled, the system generates motion data for the images used for motion detection. For example, if you select motion detection on keyframes only, the motion data is also produced for keyframes only.

The extra motion data enables the client user, via the smart search function, to quickly search for relevant recordings based on motion in the selected area of the image. The motion data is not generated for areas with privacy masks.

Motion detection threshold and exclude regions do not influence the generated motion data.

You specify the default setting of generating smart search data for cameras on the **Tools > Options > General** tab.

Specify exclude regions

You can disable motion detection in specific areas of a camera view.

Disabling motion detection in specific areas helps you avoid detection of irrelevant motion, for example if the camera covers an area where a tree is swaying in the wind or where cars regularly pass by in the background.

When you use exclude regions with PTZ cameras and you pan/tilt/zoom the camera, the excluded area does **not** move accordingly because the area is locked to the camera image, and not the object.

1. To use exclude regions, select the *Use exclude regions* check box.
A grid divides the preview image into selectable sections.
2. To define exclude regions, drag the mouse pointer over the required areas in the preview image while you press the left mouse button. Right mouse button clears a grid section.

You can define as many exclude regions as needed. Excluded regions appear in blue.

The blue exclude areas only appear in the preview image on the *Motion* tab, not in any other preview images in the Management Client or access clients.

Client

About clients

The Client section of the Management Client consists of:

Name	Description
View groups	View groups are used solely when running Ocularis Client in Limited Mode. Users are granted access to View groups via their role.
Management Client profiles	To differentiate Management Client administrator users, you can create Management Client profiles, prioritize these and customize their profiles as needed for the different tasks at hand.
NetMatrix	NetMatrix is a feature for distributing video remotely and is typically not used if you are using Ocularis as Ocularis inherently supports this feature. If you use Ocularis Client in Limited Mode, you can use NetMatrix to push video from any camera on your system's network to anyone running Ocularis Client in Limited Mode.

View groups

About view groups

The way in which the system presents video from one or more cameras in clients is called a view. A view group is a container for one or more logical groups of such views.

When using Ocularis, view groups are configured in the *Ocularis Administrator* application. View groups described here are only for when you use Ocularis Client in Limited Mode and bypass the Base.

About view groups and roles

When using Ocularis, view groups are configured in the *Ocularis Administrator* application. View groups described here are only for when you use Ocularis Client in Limited Mode and bypass the Base.

By default, each role you define in the Management Client is also created as a view group. When you add a role in the Management Client, the role by default appears as a view group for use in Ocularis Client in Limited Mode.

- You can assign a view group based on a role to users/groups assigned to the relevant role. You may change these view group rights by setting this up in the role afterwards.
- A view group based on a role carries the role's name.

Example: If you create a role with the name *Building A Security Staff*, it appears in Ocularis Client as a view group called *Building A Security Staff*.

In addition to the view groups you get when adding roles, you may create as many other view groups as you like. You can also delete view groups, including those automatically created when adding roles.

- Even if a view group is created each time you add a role, view groups do not have to correspond to roles. You can add, rename or remove any of your view groups if required.

Note that if you rename a View group, client users already connected must log out and log in again before the name change is visible.

Add a view group

1. Right-click **View Groups**, and select *Add View Group*. This opens the *Add View Group* dialog box.
2. Type the name and an optional description of the new view group and click *OK*.

Note: No roles have the right to use the newly added view group until you have specified such rights. If you have specified which roles that can use the newly added view group, already connected client users with the relevant roles must log out and log in again before they can see the view group.

When using Ocularis, view groups are configured in the *Ocularis Administrator* application. View groups described here are only for when you use Ocularis Client in Limited Mode and bypass the Base.

Management Client profiles

About Management Client profiles

Management Client profiles allow system administrators to modify the Management Client user interface. Associate Management Client profiles with roles to limit the user interface to represent the functionality available for each administrator role.

To associate a role with a management client profile, see the Role Settings' Info tab (see "Info tab (roles)" on page 106). Note that Management Client profiles only handle the visual representation of system functionality, not the actual access to it.

To limit the overall access to system functionality for a role, see the Role Settings' Overall Security tab (see "Overall Security tab (roles)" on page 107).

You can change settings for the visibility of all Management Client elements. By default, the Management Client profile can see all functionality in the Management Client.

- To limit visibility of functionality, clear the check boxes for the relevant functionality in order to remove the functionality visually from the Management Client for any Management Client user with a role associated with this Management Client profile.

Add and configure a Management Client profile

If you do not want to use the default profile, you can create a Management Client profile before you can configure it.

1. Right-click *Management Client Profiles*.
2. Select *Add Management Client Profile*.
3. In the *Add Management Client Profile* dialog box, type a name and description of the new profile and click **OK**.
4. In the **Overview** pane, click the profile you created to configure it.
5. On the **Profile** tab, select or clear functionality from the Management Client profile.

Copy a Management Client profile

If you have a Management Client profile with settings that you would like to reuse, you can copy an already existing profile and make minor adjustments to the copy instead of creating a new profile from scratch.

1. Click *Management Client Profile*, right-click the profile in the **Overview** pane, select *Copy Management Client Profile*.
2. In the dialog box that appears, give the copied profile a new unique name and description. Click **OK**.
3. In the **Overview** pane, click the profile and go to the **Info** tab or **Profile** tab to configure the profile.

Management Client profile properties

INFO TAB (MANAGEMENT CLIENT PROFILES)

On the **Info** tab, you can set the following for Management Client profiles:

Component	Requirement
Name	Enter a name for the Management Client profile.
Priority	Use the up and down arrows to set a priority for the Management Client profile.
Description	Enter a description for the profile. This is optional.
Roles using the Management Client profile	This field shows the roles that you have associated with the Management Client profile. You cannot edit this.

PROFILE TAB (MANAGEMENT CLIENT PROFILES)

On the **Profile** tab, you can enable or disable the visibility of the following elements from the Management Client's user interface:

Navigation

In this section, decide if an administrator user associated with the Management Client profile is allowed to see the various features and functionality located in the **Navigation** pane.

Navigation element	Description
Basics	Allows the administrator user associated with the Management Client profile to see License Information and Site Information .
Remote Connect Services	Allows the administrator user associated with the Management Client profile to see Axis One-click Camera Connection .
Servers	Allows the administrator user associated with the Management Client profile to see Recording Servers and Failover Servers .
Devices	Allows the administrator user associated with the Management Client profile to see Cameras , Microphones , Speakers , Metadata , Input and Output .
Client	Allows the administrator user associated with the Management Client profile to see the nodes for View Groups , Management Client Profiles and NetMatrix .
Rules and Events	Allows the administrator user associated with the Management Client profile to see Rules , Time Profiles , Notification Profiles , and User-defined Events .
Security	Allows the administrator user associated with the Management Client profile to see Roles and Basic Users .
System Dashboard	Allows the administrator user associated with the Management Client profile to see System Monitor , Current Tasks and Configuration Reports .
Server Logs	Allows the administrator user associated with the Management Client profile to see System Log , Audit Log and Rule Log .

Details

In this section, decide if an administrator user associated with the Management Client profile is allowed to see the various tabs for a specific device channel, for example the **Settings** tab or **Record** tab for cameras.

Device channel	Description
Cameras	Allows the administrator user associated with the Management Client profile to see some or all camera-related settings and tabs.
Microphones	Allows the administrator user associated with the Management Client profile to see some or all microphone-related settings and tabs.
Speakers	Allows the administrator user associated with the Management Client profile to see some or all speaker-related settings and tabs.
Metadata	Allows the administrator user associated with the Management Client profile to see some or all metadata-related settings and tabs.
Input	Allows the administrator user associated with the Management Client profile to see some or all input-related settings and tabs.
Output	Allows the administrator user associated with the Management Client profile to see some or all output-related settings and tabs.

Tools Menu

In this section, decide if an administrator user associated with the Management Client profile is allowed to see the elements that are part of the **Tools** menu.

Tool Menu option	Description
Registered Services	Allows the administrator user associated with the Management Client profile to see Registered Services .
OnSSI Compatible Recording Servers	Allows the administrator user associated with the Management Client profile to see OnSSI Compatible Recording Servers .
Effective Roles	Allows the administrator user associated with the Management Client profile to see Effective Roles .
Options	Allows the administrator user associated with the Management Client profile to see Options .

Federated Sites

In this section, decide if an administrator user associated with the Management Client profile is allowed to see the Federated Sites Hierarchy pane.

NetMatrix

About NetMatrix

With Ocularis, NetMatrix is not used as its functionality is inherently supported. However, NetMatrix may be used if you use Ocularis Client in Limited Mode.

- With NetMatrix, you can send video from any camera on a network operating your system to NetMatrix-recipients. A NetMatrix recipient is a computer that can display NetMatrix-triggered video.

To see a list of NetMatrix recipients configured in the Management Client, expand *Client* in the **Site Navigation** pane, then select **NetMatrix**. A list of NetMatrix configurations is displayed in the **Properties** pane.

Each NetMatrix recipient must be configured to receive NetMatrix-triggered video.

Add NetMatrix recipients

To add an existing NetMatrix recipient through the Management Client:

1. Expand **Clients**, then select **NetMatrix**.
2. Right-click **NetMatrix Configurations** and select **Add NetMatrix**.
3. Fill out the fields in the **Add NetMatrix** dialog box.
4. In the **Address** field enter the IP address or the host name of the required NetMatrix recipient.
5. In the **Port** field enter the port number used by the NetMatrix recipient installation. You can find the port number and password in this way: For a NetMatrix application, go to the *NetMatrix Configuration* dialog box.
6. Click **OK**.

You can now use the NetMatrix recipient in rules.

Note: Your system does not verify that the specified port number or password is correct or that the specified port number, password, or type corresponds with the actual NetMatrix recipient. Make sure that you enter the correct information.

Define rules sending video to NetMatrix recipients

To send video to NetMatrix recipients you must include the NetMatrix recipient in a rule that triggers the video transmission to the related NetMatrix recipient. To do so:

1. In the **Site Navigation** pane, Expand **Rules and Events > Rules**. Right-click **Rules** to open the *Manage Rule* wizard. In the first step, select a rule type and in the second step, a condition.
2. In *Manage Rule*'s step 3 (*Step 3: Actions*) select the *Set NetMatrix to view <devices>* action.
3. Click the NetMatrix link in the initial rule description.
4. In the *Select NetMatrix Configuration* dialog box, select the relevant NetMatrix-recipient, and click **OK**.
5. Click the *devices* link in the initial rule description, and select from which cameras you would like to send video to the NetMatrix-recipient, then click **OK** to confirm your selection.
6. Click *Finish* if the rule is complete or define if required additional actions and/or a stop action.

If you delete a NetMatrix-recipient, any rule that includes the NetMatrix-recipient stops working.

Rules and events

About rules and events

Rules are a central element in your system. Rules determine highly important settings, such as when cameras should record, when PTZ cameras should patrol, when notifications should be sent, etc.



Perform an action on [Motion Start](#)
from [Camera 2](#)
start recording [3 seconds before](#) on [the device on which event occurred](#)

Perform stop action on [Motion End](#)
from [Camera 2](#)
stop recording [immediately](#)

Example: A rule specifying that a particular camera should begin recording when it detects motion.

Events are central elements when using the *Manage Rule* wizard. In the wizard, events are primarily used for triggering actions. For example, you can create a rule which specifies that in the *event* of detected motion, the surveillance system should take the *action* of starting recording of video from a particular camera.

Two types of conditions can trigger rules:

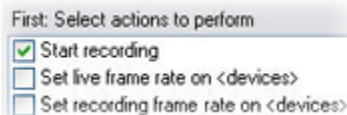
Name	Description
Events	When events occur on the surveillance system, for example when motion is detected, when the system receives input from external sensors.
Time	When you enter specific periods of time, for example <i>Thursday 16th August 2007 from 07.00 to 07.59, or every Saturday and Sunday</i> .

You can work with the following under *Rules and Events*:

- **Rules:** Rules are a central element in the system. The behavior of your surveillance system is to a very large extent determined by rules. When creating a rule, you can work with all types of events.
- **Time profiles:** Time profiles are periods of time defined in the Management Client. You use them when you create rules in the Management Client, for example to create a rule which specifies that a certain action should take place within a certain time profile.
- **Notification profiles:** You can use notification profiles to set up ready-made email notifications, which can automatically be triggered by a rule, for example when a particular event occurs.
- **User-defined events:** User-defined events are custom-made events that makes it possible for users to manually trigger events in the system or react to inputs from the system.

About actions and stop actions

When you add rules in the *Manage Rule* wizard, you can select between different actions:



Example: Selecting actions

Some of the actions require a stop action. **Example:** If you select the action *Start recording*, recording starts and potentially continues indefinitely. As a result, the action *Start recording* has a mandatory stop action called *Stop recording*.

The *Manage Rule* wizard makes sure you specify stop actions when necessary.

Each type of action from the system is described. You may have more actions available if your system installation uses add-on products or vendor-specific plug-ins. For each type of action, stop action information is listed if relevant:

Action	Description
Start recording on <devices>	<p>Start recording and saving data in the database from the selected devices.</p> <p>When you select this type of action, the <i>Manage Rule</i> wizard prompts you to specify:</p> <p>When recording should start. This happens either immediately or a number of seconds before the triggering event/beginning of the triggering time interval and on which devices the action should take place.</p> <p>This type of action requires that you have enabled recording on the devices to which the action are linked. You can only save data from before an event or time interval if you have enabled pre-buffering for the relevant devices. You enable recording and specify pre-buffering settings for a device on the Record tab.</p> <p>Stop action required: This type of action requires one or more stop actions. In one of the following steps, the wizard automatically prompts you to specify the stop action: Stop recording.</p> <p>Without this stop action, recording would potentially continue indefinitely. You also have the option of specifying further stop actions.</p>
Start feed on	Begin data feed from devices to the system. When the feed from a device is started,

Action	Description
<devices>	<p>data is transferred from the device to the system, in which case you may view and record, depending on the data type.</p> <p>When you select this type of action, the <i>Manage Rule</i> wizard prompts you to specify on which devices to start the feeds. Your system includes a default rule which ensures that feeds are always started on all cameras.</p> <p>Stop action required: This type of action requires one or more stop actions. In one of the following steps, the wizard automatically prompts you to specify the stop action: Stop feed.</p> <p>You can also specify further stop actions.</p> <p>Note that using the mandatory stop action <i>Stop feed</i> to stop the feed from a device means that data is no longer transferred from the device to the system, in which case live viewing and recording of video, for example, is no longer possible. However, a device on which you have stopped the feed can still communicate with the recording server, and you can start the feed again automatically through a rule, as opposed to when you manually have disabled the device.</p> <p>Important: While this type of action enables access to selected devices' data feeds, it does not guarantee that data is recorded, as you must specify recording settings separately.</p>
Set live frame rate on <devices>	<p>Sets a particular frame rate to use when the system displays live video from the selected cameras that substitutes the cameras' default frame rate. Specify this on the Settings tab.</p> <p>When you select this type of action, the <i>Manage Rule</i> wizard prompts you to specify which frame rate to set, and on which devices. Always verify that the frame rate you specify is available on the relevant cameras.</p> <p>Stop action required: This type of action requires one or more stop actions. In one of the following steps, the wizard automatically prompts you to specify the stop action: Restore default live frame rate.</p> <p>Without this stop action, the default frame rate would potentially never be restored. You also have the option of specifying further stop actions.</p>
Set recording frame rate on <devices>	<p>Sets a particular frame rate to use when the system saves recorded video from the selected cameras in the database, instead of the cameras' default recording frame rate.</p> <p>When you select this type of action, the <i>Manage Rule</i> wizard prompts you to specify which recording frame rate to set, and on which cameras.</p> <p>You can only specify a recording frame rate for JPEG, a video codec with which each frame is separately compressed into a JPEG image. This type of action also requires that you have enabled recording on the cameras to which the action is linked. You enable recording for a camera on the <i>Record</i> tab. The maximum frame rate you can specify depends on the relevant camera types, and on their selected image resolution.</p> <p>Stop action required: This type of action requires one or more stop actions. In one of the following steps, the wizard automatically prompts you to specify the stop action: Restore default recording frame rate.</p> <p>Without this stop action, the default recording frame rate would potentially never be restored. You also have the option of specifying further stop actions.</p>
Set recording frame rate to all frames for H.264/MPEG4 on <devices>	<p>Sets the frame rate to record all frames when the system saves recorded video from the selected cameras in the database, instead of keyframes only. Enable the recording keyframes only function on the <i>Record</i> tab.</p> <p>When you select this type of action, the <i>Manage Rule</i> wizard prompts you to select which devices the action should apply for.</p> <p>You can only enable keyframe recording for H.264 and MPEG4. This type of action also requires that you have enabled recording on the cameras to which the action is linked. You enable recording for a camera on the <i>Record</i> tab.</p> <p>Stop action required: This type of action requires one or more stop actions. In one of</p>

Action	Description
	<p>the following steps, the wizard automatically prompts you to specify the stop action:</p> <p>Restore default recording frame rate of keyframes for H.264/MPEG4</p> <p>Without this stop action, the default setting would potentially never be restored. You also have the option of specifying further stop actions.</p>
Start patrolling on <device> using <profile> with PTZ priority <priority>	<p>Begins PTZ patrolling according to a particular patrolling profile for a particular PTZ camera with a particular priority. This is an exact definition of how patrolling should be carried out, including the sequence of preset positions, timing settings, and more.</p> <p>If you have upgraded your system from an older version of the system, the old values (<i>Very Low, Low, Medium, High</i> and <i>Very High</i>) have been translated as follows:</p> <ul style="list-style-type: none"> ○ Very Low = 1000 ○ Low = 2000 ○ Medium = 3000 ○ High = 4000 ○ Very High = 5000 <p>When you select this type of action, the <i>Manage Rule</i> wizard prompts you to select a patrolling profile. You can only select one patrolling profile on one device and you cannot select several patrolling profiles.</p> <p>This type of action requires that the devices to which the action is linked are PTZ devices.</p> <p>You must define at least one patrolling profile for the device(s). You define patrolling profiles for a PTZ camera on the <i>Patrolling</i> tab.</p> <p>Stop action required: This type of action requires one or more stop actions. In one of the following steps, the wizard automatically prompts you to specify the stop action:</p> <p>Stop patrolling</p> <p>Without this stop action, patrolling would potentially never stop. You can also specify further stop actions.</p>
Pause patrolling on <devices>	<p>Pauses PTZ patrolling. When you select this type of action, the <i>Manage Rule</i> wizard prompts you to specify the devices on which to pause patrolling.</p> <p>This type of action requires that the devices to which the action is linked are PTZ devices.</p> <p>You must define at least one patrolling profile for the device(s). You define patrolling profiles for a PTZ camera on the <i>Patrolling</i> tab.</p> <p>Stop action required: This type of action requires one or more stop actions. In one of the following steps, the wizard automatically prompts you to specify the stop action:</p> <p>Resume patrolling</p> <p>Without this stop action, patrolling would potentially pause indefinitely. You have also the option of specifying further stop actions.</p>
Move <device> to <preset> position with PTZ priority <priority>	<p>Moves a particular camera to a particular preset position - however always according to priority. When selecting this type of action, the <i>Manage Rule</i> wizard prompts you to select a preset position. Only one preset position on one camera can be selected. It is not possible to select several preset positions.</p> <p>This type of action requires that the devices to which the action is linked are PTZ devices.</p> <p>This action requires that you have defined at least one preset position for those</p>

Action	Description
	<p>devices. You define preset positions for a PTZ camera on the <i>Presets</i> tab.</p> <p>No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.</p>
Move to default preset on <devices> with PTZ priority <priority>	<p>Moves one or more particular cameras to their respective default preset positions - however always according to priority. When you select this type of action, the <i>Manage Rule</i> wizard prompts you to select which devices the action should apply for.</p> <p>This type of action requires that the devices to which the action is linked are PTZ devices.</p> <p>This action requires that you have defined at least one preset position for those devices. You define preset positions for a PTZ camera on the <i>Presets</i> tab.</p> <p>No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.</p>
Set device output to <state>	<p>Sets an output on a device to a particular state (activated or deactivated). When you select this type of action, the <i>Manage Rule</i> wizard prompts you to specify which state to set, and on which devices.</p> <p>This type of action requires that the devices to which the action is linked each have at least one external output unit connected to an output port.</p> <p>No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.</p>
Send notification to <profile>	<p>Sends a notification, using a particular notification profile. When you select this type of action, the <i>Manage Rule</i> wizard prompts you to select a notification profile, and which devices to include pre-alarm images from. You can only select one notification profile and you cannot select several notification profiles. Note that a single notification profile may contain several recipients.</p> <p>You can also create more rules to the same event and send different notifications to each of the notification profiles. You can copy and re-use the content of rules by right-clicking a rule in the Rules list.</p> <p>This type of action requires that you have defined at least one notification profile. Pre-alarm images are only included if you have enabled the <i>Include images</i> option for the relevant notification profile.</p> <p>No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.</p>
Make new <log entry>	<p>Generates an entry in the rule log. When selecting this type of action, the <i>Manage Rule</i> wizard prompts you to specify a text for the log entry. When you specify the log text, you can insert variables, such as \$DeviceName\$, \$EventName\$, into the log message.</p> <p>No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.</p>

Action	Description
Start plug-in on <devices>	<p>Starts one or more plug-ins. When you select this type of action, the <i>Manage Rule</i> wizard prompts you to select required plug-ins, and on which devices to start the plug-ins.</p> <p>This type of action requires that you have at least one or more plug-ins installed on your system.</p> <p>No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.</p>
Stop plug-in on <devices>	<p>Stops one or more plug-ins. When you select this type of action, the <i>Manage Rule</i> wizard prompts you to select required plug-ins, and on which devices to stop the plug-ins.</p> <p>This type of action requires that you have at least one or more plug-ins installed on your system.</p> <p>No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.</p>
Apply new settings on <devices>	<p>Changes device settings on one or more devices. When you select this type of action, the <i>Manage Rule</i> wizard prompts you to select relevant devices, and you can define the relevant settings on the devices you have specified.</p> <p>If you define settings for more than one device, you can only change settings that are available for all of the specified devices.</p> <p>Example: You specify that the action should be linked to Device 1 and Device 2. Device 1 has the settings A, B and C, and Device 2 has the settings B, C and D. In this case, you can only change the settings that are available for both devices, namely settings B and C.</p> <p>No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.</p>
Set NetMatrix to view <devices>	<p>Makes video from the selected cameras appear on a computer capable of displaying NetMatrix-triggered video such as a computer on which you have installed the NetMatrix application.</p> <p>When you select this type of action, the <i>Manage Rule</i> wizard prompts you to select a NetMatrix recipient, and one or more devices from which to display video on the selected NetMatrix recipient.</p> <p>This type of action allows you to select only a single NetMatrix recipient at a time. If you want to make video from the selected devices appear on more than one NetMatrix recipient, you should create a rule for each required NetMatrix recipient. By right-clicking a rule in the Rules list, you can copy and re-use the content of rules. This way, you can avoid having to create near-identical rules from scratch.</p> <hr/> <p>As part of the configuration on the NetMatrix recipients themselves, users must specify the port number and password required for the NetMatrix communication. Make sure that the users have access to this information. The users must typically also define the IP addresses of allowed hosts from which commands regarding display of NetMatrix-triggered video is accepted. In that case, the users must also know the IP address of the management server, or any router or firewall used.</p> <hr/>
Send SNMP trap	<p>Generates a small message which logs events on selected devices. The text of SNMP traps are auto-generated and cannot be customized. It can contain the source type and name of the device on which the event occurred.</p> <p>No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.</p>

Action	Description
Retrieve and store remote recordings from <devices>	Retrieves and stores remote recordings from selected devices (that support edge recording) in a specified period before and after the triggering event. Note that this rule is independent of the <i>Automatically retrieve remote recordings when connection is restored</i> setting. No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.
Retrieve and store remote recordings between <start and end time> from <devices>	Retrieves and stores remote recordings in a specified period from selected devices (that support edge recording). Note that this rule is independent of the <i>Automatically retrieve remote recordings when connection is restored</i> setting. No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.
Save attached image	Ensures that when an image is received from the Images Received event (sent via SMTP email from a camera), it is saved for future usage. In future, other events can possibly also trigger this action. No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.
Activate archiving on <archives>	Starts archiving on one or more archives. When you select this type of action, the <i>Manage Rule</i> wizard prompts you to select relevant archives. No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.
On <site> trigger <user-defined event>	Relevant mostly within OnSSI Federated Architecture, but you can also use this in a single site setup. Use the rule to trigger a user-defined event on a site, normally a remote site within a federated hierarchy. No mandatory stop action: This type of action does not require a stop action. You can specify optional stop actions to be performed on either an event or after a period of time.

Events overview

When you add an event-based rule in the *Manage Rule* wizard, you can select between a number of different event types. In order for you to get a good overview, events you can select are listed in groups according to whether they are:

Hardware:

Some hardware is capable of creating events themselves, for example to detect motion. You can use these as events but you must configure them on the hardware before you can use them in the system. You may only be able to use the events listed on some hardware as not all types of cameras can detect tampering or temperature changes.

Hardware - Configurable events:

Configurable events from hardware are automatically imported from device drivers. This means that they vary from hardware to hardware and are not documented here. Configurable events are not triggered until you have added them to the system and configured them on the **Event** tab for hardware. Some of the configurable events also require that you configure the camera (hardware) itself.

Hardware - Predefined events:

Event	Description
Communication Error (Hardware)	Occurs when a connection to a the hardware is lost.
Communication Started (Hardware)	Occurs when communication with the hardware is successfully established.
Communication Stopped (Hardware)	Occurs when communication with the hardware is successfully stopped.

Devices - Configurable events:

Configurable events from devices are automatically imported from device drivers. This means that they vary from device to device and are not documented here. Configurable events are not triggered until you have added them to the system and configured them on the **Event** tab on a device.

Devices - Predefined events:

Event	Description
Communication Error (Device)	Occurs when a connection to a device is lost, or when an attempt is made to communicate with a device, and the attempt is unsuccessful.
Communication Started (Device)	Occurs when communication with a device is successfully established.
Communication Stopped (Device)	Occurs when communication with a device is successfully stopped.
Feed Overflow Started	<p>Feed overflow (media overflow) occurs when a recording server cannot process received data as quickly as specified in the configuration and therefore is forced to discard some recordings.</p> <p>If the server is healthy, feed overflow usually happens because of slow disk writes. You can resolve this either by reducing the amount of data written, or by improving the storage system's performance. Reduce the amount of written data by reducing frame rates, resolution or image quality on your cameras, but this may degrade recording quality. If you are not interested in that, instead improve your storage system's performance by installing extra drives to share the load or by installing faster disks or controllers.</p> <p>You can use this event to trigger actions that helps you avoid the problem, for example, to lower the recording frame rate.</p>
Feed Overflow Stopped	Occurs when feed overflow (see description of the <i>Feed Overflow Started</i> event) ends.
Live Client Feed Requested	<p>Occurs when client users request a live stream from a device.</p> <p>The event occurs upon the request even if the client user's request later turns out to be unsuccessful, for example because the client user does not have the rights required for viewing the requested live feed or because the feed is for some reason stopped.</p>
Live Client Feed Terminated	Occurs when client users no longer request a live stream from a device.
Manual Recording Started	<p>Occurs when a client user starts a recording session for a camera.</p> <p>The event is triggered even if the device already is being recorded via rule actions.</p>

Event	Description
Manual Recording Stopped	Occurs when a client user stops a recording session for a camera. If the rule system also have started a recording session it continues recording even after the manual recording is stopped.
Motion Started	Occurs when the system detects motion in video received from cameras. This type of event requires that the system's motion detection is enabled for the cameras to which the event is linked. In addition to the system's motion detection, some cameras can detect motion themselves and trigger the <i>Motion Started (HW)</i> event, but it depends on the configuration of the camera hardware and in the system. See Hardware - Configurable events above.
Motion Stopped	Occurs when motion is no longer detected in received video. See also the description of the <i>Motion Started</i> event. This type of event requires that the system's motion detection is enabled for the cameras to which the event is linked. In addition to the system's motion detection, some cameras can detect motion themselves and trigger the Motion Stopped (HW) event, but it depends on the configuration of the camera hardware and in the system. See Hardware - Configurable events above.
Output Activated	Occurs when an external output port on a device is activated. This type of event requires that at least one device on your system supports output ports.
Output Changed	Occurs when the state of an external output port on a device is changed. This type of event requires that at least one device on your system supports output ports.
Output Deactivated	Occurs when an external output port on a device is deactivated. This type of event requires that at least one device on your system supports output ports.
PTZ Manual Session Started	Occurs when a manually operated PTZ session (as opposed to a PTZ session based on scheduled patrolling or automatically triggered by an event) is started on a camera. This type of event requires that the cameras to which the event is linked are PTZ cameras.
PTZ Manual Session Stopped	Occurs when a manually operated PTZ session (as opposed to a PTZ session based on scheduled patrolling or automatically triggered by an event) is stopped on a camera. This type of event requires that the cameras to which the event is linked are PTZ cameras.
Recording Started	Occurs whenever recording is started. There is a separate event for manual recording started.

Event	Description
Recording Stopped	Occurs whenever recording is stopped. There is a separate event for manual recording stopped.
Settings Changed	Occurs when settings on a device are successfully changed.
Settings Changed Error	Occurs when an attempt is made to change settings on a device, and the attempt is unsuccessful.

External events - Predefined events:

Event	Description
Request Start Recording	Activated when start recordings are requested.
Request Stop Recording	Activated when stop recordings are requested.

External events - User-defined events:

A number of events custom made to suit your system may also be selectable. You can use such user-defined events for:

- Making it possible for client users to manually trigger events while viewing live video in the clients.
- Countless other purposes. For example, you may create user-defined events which occur if a particular type of data is received from a device.

See About user-defined events (on page 103) for more information.

Recording servers:

Event	Description
Archive Available	Occurs when an archive for a recording server becomes available after having been unavailable (see <i>Archive Unavailable</i>).
Archive Unavailable	Occurs when an archive for a recording server becomes unavailable, for example if the connection to an archive located on a network drive is lost. In such cases, you cannot archive recordings. You can use the event to, for example, trigger an alarm or a notification profile so that an email notification is automatically sent to relevant people in your organization.
Archive Not Finished	Occurs when an archive for a recording server is not finished with the last archiving round when the next is scheduled to start.

Event	Description
Database Disk Full	Occurs when a database disk is full. A database disk is considered to be full when there is less than 5GB of space is left on the disk: The oldest data in a database is always auto-archived (or deleted if no next archive is defined) when less than 5GB of space is free. If less than 1GB space is free, data is deleted even if a next archive is defined. A database always requires 250MB of free space. If this limit is reached (if data is not deleted fast enough), no more data is written to the database until enough space has been freed. The actual maximum size of your database is the amount of gigabytes you specify, minus 5GB.
Database Full - Auto Archive	Occurs when an archive for a recording server is full and needs to auto-archive to an archive in the storage.
Database Repair	Occurs if a database becomes corrupted, in which case the system automatically attempts two different database repair methods: a fast repair and a thorough repair.
Database Storage Available	Occurs when a storage for a recording server becomes available after having been unavailable (see <i>Database Storage Unavailable</i>). You can, for example, use the event to start recording if it has been stopped by a <i>Database Storage Unavailable</i> event.
Database Storage Unavailable	Occurs when a storage for a recording server becomes unavailable, for example if the connection to a storage located on a network drive is lost. In such cases, you cannot archive recordings. You can use the event to, for example, stop recording, trigger an alarm or a notification profile so an e-mail notification is automatically sent to relevant people in your organization.
Failover Started	Occurs when a failover recording server takes over from a recording server. See About failover recording servers (on page 131).
Failover Stopped	Occurs when a recording server becomes available again, and can take over from a failover recording server.

Rules

About rules

Rules specify actions to carry out under particular conditions. Example: When motion is detected (condition), a camera should begin recording (action).

The following are *examples* of what you can do with rules:

- Start and stop recording
- Set non-default live frame rate
- Set non-default recording frame rate
- Start and stop PTZ patrolling
- Pause and resume PTZ patrolling
- Move PTZ cameras to specific positions
- Set output to activated/deactivated state
- Send notifications via e-mail

- Generate log entries
- Generate events
- Apply new device settings, for example a different resolution on a camera
- Make video appear in NetMatrix recipients
- Start and stop plug-ins
- Start and stop feeds from devices

Stopping a device means that video is no longer transferred from the device to the system, in which case you cannot view live video nor record video. In contrast, a device on which you have stopped the feed can still communicate with the recording server, and you can start the feed from the device automatically through a rule, as opposed to when the device is manually disabled in the Management Client.

Important: Some rule content may require that certain features are enabled for the relevant devices. For example, a rule specifying that a camera should record does not work as intended if recording is not enabled for the relevant camera. Before creating a rule, OnSSI recommends that you verify that the devices involved can perform as intended.

About default rules

Your system includes a number of default rules that you can use basic features without needing to set anything up. You can deactivate or modify the default rules as you need. If you modify or deactivate the default rules, your system may not work as desired nor guarantee that video feeds or audio feeds are automatically fed to the system.

Default rule	Description
<i>Goto Preset when PTZ is done</i>	Ensures that PTZ cameras go to their respective default preset positions after you have operated them manually. This rule is not enabled by default. Even when you have enabled the rule, you must have defined default preset positions for the relevant PTZ cameras in order for the rule to work. You do this on the <i>Presets</i> tab.
<i>Record on Motion</i>	Ensures that as long as motion is detected in video from cameras, the video is recorded, provided recording is enabled for the relevant cameras. Recording is by default enabled. While the default rule specifies recording based on detected motion, it does not guarantee that the system records video, as you may have disabled individual cameras' recording for one or more cameras. Even when you have enabled recording, remember that the quality of recordings may be affected by individual camera's recording settings.
<i>Record on Request</i>	Ensures that video is recorded automatically when an external request occurs, provided recording is enabled for the relevant cameras. Recording is enabled by default. The request is always triggered by a system integrating externally with your system, and the rule is primarily used by integrators of external systems or plug-ins.
<i>Start Audio Feed</i>	Ensures that audio feeds from all connected microphones and speakers are automatically fed to the system. While the default rule enables access to connected microphones' and speakers' audio feeds immediately upon installing the system, it does not guarantee that audio is recorded, as you must specify recording settings separately.

Default rule	Description
Start Feed	Ensures that video feeds from all connected cameras are automatically fed to the system. While the default rule enables access to connected cameras' video feeds immediately upon installing the system, it does not guarantee that video is recorded, as cameras' recording settings must be specified separately.
Start Metadata Feed	Ensures that data feeds from all connected cameras are automatically fed to the system. While the default rule enables access to connected cameras' data feeds immediately upon installing the system, it does not guarantee that data is recorded, as cameras' recording settings must be specified separately.

Recreate default rules

If you accidentally delete any of the default rules, you can recreate them by using the following content:

Default rule	Text to type
Goto preset when PTZ is done	Perform an action on PTZ Manual Session Stopped from All Cameras Move immediately to default preset on the device on which event occurred
Record on Motion	Perform an action on Motion Started from All Cameras start recording three seconds before on the device on which event occurred Perform stop action on Motion Stopped from All Cameras stop recording three seconds after
Record on Request	Perform an action on Request Start Recording from External start recording immediately on the devices from metadata Perform stop action on Request Stop Recording from External stop recording immediately
Start Audio Feed	Perform an action in a time interval always start feed on All Microphones, All Speakers Perform an action when time interval ends stop feed immediately
Start Feed	Perform an action in a time interval always start feed on All Cameras Perform an action when time interval ends stop feed immediately
Start Metadata Feed	Perform an action in a time interval always start feed on All Metadata Perform an action when time interval ends stop feed immediately

About validating rules

You can validate the content of an individual rule or all rules in one go. When you create a rule, the **Manage Rule** wizard ensures that all of the rule's elements make sense. When a rule has existed for some time, one or more of the rule's elements may have been affected by other configuration, and the rule may no longer work. For example, if a rule is triggered by a particular time profile, the rule does not work if you have deleted that time profile or if you no longer have permissions to it. Such unintended effects of configuration may be hard to keep an overview of.

Rule validation helps you keep track of which rules have been affected. Validation takes place on a per-rule basis and each rule is validated by themselves. You cannot validate rules against each other, for example in order to see whether one rule conflicts with another rule, not even if you use the *Validate All Rules* feature.

Note that you cannot validate whether configuration of prerequisites outside the rule itself may prevent the rule from working. For example, a rule specifying that recording should take place when motion is detected by a particular camera validates OK if the elements in the rule itself are correct, even if motion detection, which is enabled on a camera level, not through rules, has not been enabled for the relevant camera.

You validate an individual rule or all rules in one go by right-clicking the rule you want to validate and select *Validate Rule* or *Validate All Rules*. A dialog box informs you whether the rule(s) validated successfully or not. If you chose to validate more than one rule and one or more rules did not succeed, the dialog box lists the names of the affected rules.



About rule complexity

Your exact number of options depends on the type of rule you want to create, and on the number of devices available on your system. Rules provide a high degree of flexibility: you can combine event and time conditions, specify several actions in a single rule, and very often create rules covering several or all of the devices on your system.

You can make your rules as simple or complex as required. For example, you can create very simple time-based rules:

Example	Explanation
<i>Very Simple Time-Based Rule</i>	On Mondays between 08.30 and 11.30 (time condition), Camera 1 and Camera 2 should start recording (action) when the time period begins and stop recording (stop action) when the time period ends.
<i>Very Simple Event-Based Rule</i>	When motion is detected (event condition) on Camera 1, Camera 1 should start recording (action) immediately, then stop recording (stop action) after 10 seconds. Even if an event-based rule is activated by an event on one device, you can specify that actions should take place on one or more other devices.
<i>Rule Involving Several Devices</i>	When motion is detected (event condition) on Camera 1, Camera 2 should start recording (action) immediately, and the siren connected to Output 3 should sound (action) immediately. Then, after 60 seconds, Camera 2 should stop recording (stop action), and the siren connected to Output 3 should stop sounding (stop action).
<i>Rule Combining Time, Events, and Devices</i>	When motion is detected (event condition) on Camera 1, and the day of the week is Saturday or Sunday (time condition), Camera 1 and Camera 2 should start recording (action) immediately, and a notification should be sent to the security manager (action). Then, 5 seconds after motion is no longer detected on Camera 1 or Camera 2, the 2 cameras should stop recording (stop action).

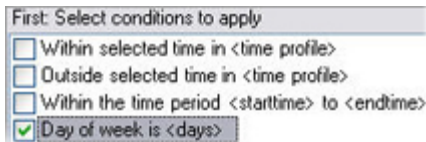
Depending on your organization's needs, it is often a good idea to create many simple rules rather than a few complex rules. Even if it means you have more rules in your system, it provides an easy way to maintain an overview of what your rules do. Keeping your rules simple also means that you have much more flexibility when it comes to deactivating/activating individual rule elements. With simple rules, you can deactivate/activate entire rules when required.

Add a rule

When you create rules, you are guided by the wizard *Manage Rule* which only lists relevant options.

It ensures that a rule does not contain missing elements. Based on your rule's content, it automatically suggests suitable stop actions, that is what should take place when the rule no longer applies, ensuring that you do not unintentionally create a never-ending rule.

1. Right-click the *Rules* item > *Add Rule*. This opens the **Manage Rule** wizard. The wizard guides you through the process of specifying the content of your rule. The wizard asks you to specify your exact requirements for the rule.
2. Specifying a name and a description of the new rule in the *Name* and *Description* fields respectively.
3. Select the relevant type of condition for the rule: either a rule which performs one or more actions when a particular event occurs, or a rule which performs one or more actions when you enter a specific period of time.
4. Click *Next* to go to the wizard's second step. On the wizard's second step, define further conditions for the rule.
5. Select one or more conditions, for example *Day of week is <day>*:



Example only. Your selections may be different

Depending on your selections, edit the rule description in the lower part of the wizard window:



Example only. Your selections may be different

Click the underlined items in **bold italics** to specify their exact content. For example, clicking the *days* link in our example lets you select one or more days of the week on which the rule should apply.

6. Having specified your exact conditions, click *Next* to move to the next step of the wizard and select which actions the rule should cover. Depending on the content and complexity of your rule, you may need to define more steps, such as stop events and stop actions. For example, if a rule specifies that a device should perform a particular action during a time interval (for example, Thursday between 08.00 and 10.30), the wizard may ask you to specify what should happen when that time interval ends.
7. Your rule is by default active once you have created it if the rule's conditions are met. If you do not want the rule to be active straight away, clear the *Active* check box.
8. Click *Finish*.

For more information, see **Perform an action on <event> and Perform an action in a time interval**.

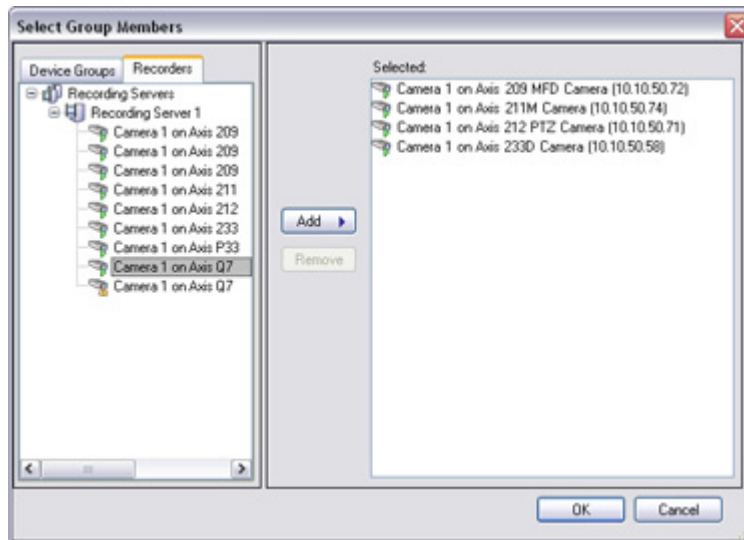
If you select a time-based rule, no more information is required on the wizard's first step.

If you select an event-based rule, the lower part of the wizard window will display an initial rule description:



Click the underlined items in the rule description in order to specify its exact content:

- **Event:** Clicking the *event* link lets you select the event which must occur in order for the rule to apply (for example *Motion Started*).
- **Devices/recording server/management server:** When you have selected the required event, clicking the *devices/recording server/management server* link lets you specify the devices on which the event should occur in order for the rule to apply. Depending on your event specification, you may be able to select from a list of cameras, inputs, outputs, etc. In this example illustration, the selectable devices are all cameras:



You specify the required devices by moving them from the *Available devices* list to the *Selected devices* list.

To move a device from the *Available devices* list to the *Selected devices* list, either select the device and click the *Add* button, double-click the device, or simply drag the device from one list to the other.

Tip: When devices are grouped into so-called device groups, you can quickly move all devices in a group simply by moving the group folder.

When the required devices are listed in the *Selected devices* list, click *OK*.

You have now specified the exact content of the first part of the rule description:

Next: Edit the rule description (click an underlined item)
 Perform an action on Motion Start
 from Blue Sector Back Door, Blue Sector Entrance

Example only; your selections may be different

Edit, copy and rename a rule

1. In the **Overview** pane, right-click the relevant rule.
2. Select either:
Edit Rule or *Copy Rule* or *Rename Rule*. The wizard *Manage Rule* opens.
3. In the wizard, rename and/or change the rule. If you selected *Copy Rule*, the wizard opens, displaying a copy of the selected rule.
4. Click *Finish*.

Deactivate and activate a rule

Your system applies a rule as soon as the rule's conditions apply which means it is active. If you do not want a rule to be active, you can deactivate the rule. When you deactivate the rule, the system does not apply the rule even if the rule's conditions apply. You can easily activate a deactivated rule later.

Deactivating a rule

1. In the **Overview** pane, select the rule.
2. Clear the *Active* check box in the **Properties** pane.
3. Click *Save* in the toolbar.

4. An icon with a red x indicates that the rule is deactivated in the *Rules* list:



Example: The added x on the icon indicates that the third rule is deactivated

Activating a rule

When you want to activate the rule again, select the rule, select the *Activate* check box, and save the setting.

Time profiles

About time profiles

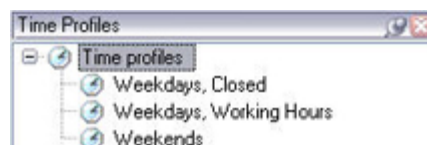
Time profiles are periods of time defined by the administrator. You can use time profiles when creating rules, for example, a rule specifying that a certain action should take place within a certain time period.

Time profiles are also assigned to roles. Per default, all roles are assigned the default time profile *Always*. This means that members of roles with this default time profile attached has no time-based limits to their user rights in the system. You can also assign an alternative time profile to a role.

Time profiles are highly flexible: you can base them on one or more single periods of time, on one or more recurring periods of time, or a combination of single and recurring times. Many users may be familiar with the concepts of single and recurring time periods from calendar applications, such as the one in Microsoft® Outlook.

Time profiles always apply in local time. This means that if your system has recording servers placed in different time zones, any actions, for example recording on cameras, associated with time profiles are carried out in each recording server's local time. Example: If you have a time profile covering the period from 08.30 to 09.30, any associated actions on a recording server placed in New York is carried out when the local time is 08.30 to 09.30 in New York, while the same actions on a recording server placed in Los Angeles is carried out some hours later, when the local time is 08.30 to 09.30 in Los Angeles.

You create and manage time profiles by expanding *Rules and Events > Time Profiles*. A *Time Profiles* list opens:



Example only

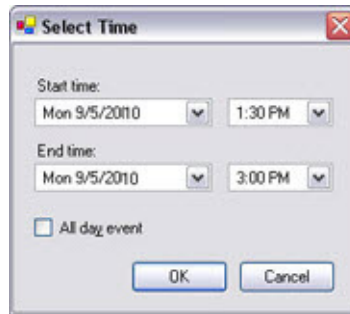
For an alternative to time profiles, see Day length time profiles (see "About day length time profiles" on page 99).

Specify a time profile

1. In the *Time Profiles* list, right-click *Time Profiles > Add Time Profile*. This opens the *Time Profile* window.
2. In the *Time Profile* window, type a name for the new time profile in the *Name* field. Optionally, type a description of the new time profile in the *Description* field.
3. In the *Time Profile* window's calendar, select either *Day View*, *Week View* or *Month View*, then right-click inside the calendar and select either *Add Single Time* or *Add Recurrence Time*.
4. When you have specified the time periods for your time profile, click *OK* in the *Time Profile* window. Your system adds your new time profile to the *Time Profiles* list. If at a later stage you wish to edit or delete the time profile, you do that from the *Time Profiles* list as well.

Add a single time

When you select *Add Single Time*, the *Select Time* window appears:

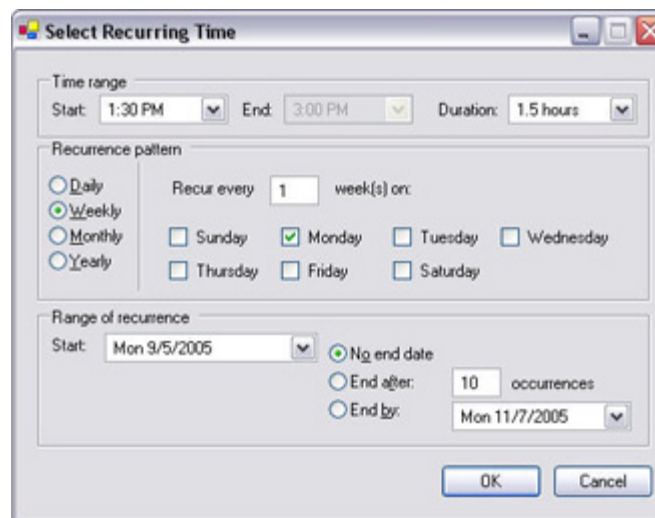


Time and date format may be different on your system

1. In the *Select Time* window, specify *Start time* and *End time*. If the time is to cover whole days, select the *All day event* box.
2. Click *OK*.

Specify a recurring time

When you select *Add Recurring Time*, the *Select Recurring Time* window appears:



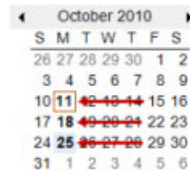
Time and date format may be different on your system

1. In the *Select Time* window, specify time range, recurrence pattern and range of recurrence.
2. Click *OK*.

A time profile can contain several periods of time. If you want your time profile to contain further periods of time, add more single times or recurring times.

Edit a time profile

1. In the **Overview** pane's *Time Profiles* list, right-click the relevant time profile, and select *Edit Time Profile*. This opens the *Time Profile* window.
2. Edit the time profile as needed. If you have made changes to the time profile, click *OK* in the *Time Profile* window. You return to the *Time Profiles* list.



You browse months by clicking the small back/forward buttons.

Note: In the *Time Profile Information* window, you can edit the time profile as needed. Remember that a time profile may contain more than one time period, and that time periods may be recurring. The small month overview in the top right corner can help you get a quick overview of the time periods covered by the time profile, as dates containing specified times are highlighted in bold.

In this example, the bold dates indicate that you have specified time periods on several days, and that you have specified a recurring time on Mondays.

About day length time profiles

When you place cameras outside, you must often lower the camera resolution, enable black/white or change other settings when it gets dark or when it gets light. The further north or south from the equator the cameras are placed, the more the sunrise and sunset time varies during the year. This makes it impossible to use normal fixed time profiles to adjust camera settings according to light conditions.

In such situations, you can create day length time profiles instead to define the sunrise and sunset in a specified geographical area. Via GPS coordinates, the system calculates the sunrise and sunset time, even incorporating daylight saving time on a daily basis. As a result, the time profile automatically follows the yearly changes in sunrise/sunset in the selected area, ensuring the profile to be active only when needed. All times and dates are based on the management servers time and date settings. You can also set a positive or negative offset (in minutes) for the start (sunrise) and end time (sunset). The offset for the start and the end time can be identical or different.

You can use day length profiles both when you create rules and roles.

Create a day length time profile

1. Expand the *Rules and Events* folder > *Time Profiles*.
2. In the *Time Profiles* list, right-click *Time Profiles*, and select *Add Day Length Time Profile*.
3. In the *Day Length Time Profile* window, fill in the needed information. To deal with transition periods between lightness and darkness, you can offset activation and deactivation of the profile. The time and the name of months are shown in the language used your computer's language/regional settings.
4. To see the location of the entered GPS coordinates in a map, click *Show Position in Browser*. This opens a browser where you can see the location.
5. Click *OK*.

Day length time profile properties

Set the following properties for day length time profile:

Name	Description
Name	The name of the profile.
Description	A description of the profile (optional).
GPS coordinates	GPS coordinates indicating the physical location of the camera(s) assigned to the profile.
Sunrise offset	Number of minutes (+/-) by which activation of the profile is offset by sunrise.

Name	Description
Sunset offset	Number of minutes (+/-) by which deactivation of the profile is offset by sunset.
Time zone	Time zone indicating the physical location of the camera(s).

Notification profiles

About notification profiles

Notification profiles allow you to set up ready-made email notifications, which can automatically be triggered by a rule, for example when a particular event occurs. You can include still images and AVI video clips in the email notifications.

The system does not support TLS (Transport Layer Security) and its predecessor SSL (Secure Socket Layer). If the sender belongs on a server that requires TLS or SSL, email notifications do not work properly. Also, you may need to disable any email scanners that could prevent the application from sending the email notifications.

Prerequisites

Before you can create notification profiles, you must specify settings for the outgoing SMTP mail server for the email notifications.

If you want the email notifications to be able to include AVI movie clips, you must also specify the compression settings to use. To do so, go to *Tools > Options*. This opens the *Options* window. Specify the **Outgoing SMTP Mail Server** on the *Mail Server* tab and the compression settings on the *AVI Generation* tab.

Add notification profiles

1. Expand *Rules and Events*, right-click *Notification Profiles > Add Notification Profile*. This opens the *Add Notification Profile* wizard.
2. Specify name and description. Click *Next*.
3. Verify that you have selected *Email*, click *Next*.
4. Specify recipient, subject, message text and time between emails:

5. To send a test email notification to the specified recipients, click *Test E-mail*.
6. To include pre-alarm still images, select *Include images*, and specify number of images, time between images and whether to embed images in emails or not.
7. To include AVI video clips, select *Include AVI*, and specify the time before and after event and frame rate.
8. Click *Finish*.

Use rules to trigger email notifications

You use the *Manage Rule* for creating rules. The wizard takes you through all relevant steps. You specify the use of a notification profile during the step on which you specify the rule's actions.

When you select the action *Send notification to <profile>*, you can select the relevant notification profile and which cameras any recordings to include in the notification profile's email notifications should come from:

Send notification to 'profile'
images from recording device

Example only. In *Manage Rule*, you click the links to make your selections

Remember that you cannot include recordings in the notification profile's email notifications unless something is actually being recorded. If you want still images or AVI video clips in the email notifications, verify that the rule specifies that recording should take place. The following example is from a rule which includes both a *Start recording* action and a *Send notification to* action:

Next: Edit the rule description (click an underlined item)

Perform an action on Input Activated
from Red Sector Door Sensor
start recording 5 seconds before on Red Sector Entrance Cam
and Send notification to 'Security: Red Sector Entrance'
images from Red Sector Entrance Cam

Perform action 10 seconds after
stop recording immediately

Notification profile (properties)

Specify the following properties for notification profiles:

Component	Requirement
Name	Type a descriptive name for the notification profile. The name appears later whenever you select the notification profile during the process of creating a rule.
Description (optional)	Type a description of the notification profile. The description appears when you pause your mouse pointer over the notification profile in the Overview pane's <i>Notification Profiles</i> list.
Recipients	Type the e-mail addresses to which the notification profile's e-mail notifications should be sent. To type more than one e-mail address, separate addresses with a semicolon. Example: aa@aaaa.aa;bb@bbbb.bb;cc@cccc.cc
Subject	Type the text you want to appear as the subject of the e-mail notification. You can insert system variables, such as <i>Device name</i> , in the subject and message text field. To insert variables, click the required variable links in the box below the field.
Message text	Type the text you want to appear in the body of the e-mail notifications. In addition to the message text, the body of each e-mail notification automatically contains this information: <ul style="list-style-type: none"> ▶ What triggered the e-mail notification. ▶ The source of any attached still images or AVI video clips
Time between e-mails	Specify required minimum time (in seconds) to pass between the sending of each e-mail notification. Examples: <ul style="list-style-type: none"> ▶ If specifying a value of 120, a minimum of 2 minutes pass between the sending of each e-mail notification, even if the notification profile is triggered again by a rule before the 2 minutes have passed. ▶ If specifying a value of 0, e-mail notifications is sent each time the notification profile is triggered by a rule. This can potentially result in a very large number of e-mail notifications being sent. If using the value 0, you should therefore carefully consider whether you want to use the notification profile in rules which are likely to be triggered frequently.
Number of images	Specify the maximum number of still images you want to include in each of the notification profile's e-mail notifications. Default is five images.
Time between images (ms)	Specify the number of milliseconds you want between the recordings presented on the included images. Example: With the default value of 500 milliseconds, the included images show recordings with half a second between them.
Time before event (sec.)	This setting is used to specify the start of the AVI file. By default, the AVI file contains recordings from 2 seconds before the notification profile is triggered. You can change this to the number of seconds you require.
Time after event (sec.)	This setting is used to specify the end of the AVI file. By default, the AVI file ends 4 seconds after the notification profile is triggered. You can change this to the number of seconds you require.
Frame rate	Specify the number of frames per second you want the AVI file to contain. Default is five frames per second. The higher the frame rate, the higher the image quality and AVI file size.
Embed images in e-mail	If selected (default), images are inserted in the body of e-mail notifications. If not, images are included in e-mail notifications as attached files.

User-defined events

About user-defined events

If the event you require is not on the *Events Overview* list, you can create your own user-defined events. Use such user-defined events to integrate other systems with your surveillance system.

With user-defined events, you can use data received from a third-party access control system as events in the system. The events can later trigger actions. This way, you can, for example, begin recording video from relevant cameras when somebody enters a building.

You can also use user-defined events for manually triggering events while viewing live video in Ocularis Client or automatically if you use them in rules. For example, when user-defined event 37 occurs, PTZ camera 224 should stop patrolling and go to preset position 18.

Through roles, you define which of your users are able to trigger the user-defined events. You can use user-defined events in two ways and at the same time if required:

Events	Description
<i>For providing the ability to manually trigger events in Ocularis Client</i>	In this case, user-defined events make it possible for end users to manually trigger events while viewing live video in Ocularis Client. When a user-defined event occurs because an Ocularis Client user triggers it manually, a rule can trigger that one or more actions should take place on the system.

No matter how you want to use user-defined events, you must add each user-defined event through the Management Client.

If you rename a user-defined event, already connected Ocularis Client users must log out and log in again before the name change is visible.

Also note that if you delete a user-defined event, this affects any rules in which the user-defined event is in use. Also, a deleted user-defined event only disappears from Ocularis Client when the Ocularis Client users log out.

Add a user-defined event

1. Expand *Rules and Events > User-defined Events*.
2. In the **Overview** pane, right-click *Events > Add User-defined Event*.
3. Type a name for the new user-defined event, and click *OK*. The newly added user-defined event now appears in the list in the **Overview** pane.
4. The user can now trigger the user-defined event manually in Ocularis Client if the user has rights to do so.

Rename a user-defined event

1. Expand *Rules and Events > User-defined Events*.
2. In the **Overview** pane, select the user-defined event.
3. In the **Properties** pane, overwrite the existing name.
4. In the toolbar, click *Save*.

Security

Roles

About roles

Roles determine which devices users can access. Roles also determine rights and handle security within the video management system. First, you add roles, then you add users and groups and finally a Management Client profile as well as other default profiles that belong to each role.

The system comes with one predefined role which you cannot delete: the *Administrators* role. Users and groups with the *Administrators* role have complete and unrestricted access to the entire system. For this reason, you cannot specify role settings for the *Administrators* role.

Users with local machine administrator rights on the computer running the management server automatically have administrator rights on the management server. Only users whom you trust as administrators of your system should have local machine administrator rights on the computer running the management server. You cannot turn this off. You add users and groups to the *Administrators* role just as with any other role. See Assign and remove users and groups to/from roles (see "Assign/remove users and groups to/from roles" on page 105).

In addition to the *Administrators* role, you can add as many roles as required to suit your needs. You may, for example, have different roles for users of Ocularis OpenSight depending on which cameras you want them to access or similar restrictions. To set up roles in your system, expand the *Security > Roles*.

About rights of a role

Available functionality depends on the recorder you are using. See Differentiate LS and ES Recorders (on page 13) for more information.

When you create a role in your system, you can give the role a number of rights to the system components or features that the relevant role can access and use.

In previous versions, your system presented a single solution to be an administrator for your system settings in the Management Client. This was through a default full administrator role with rights to see and change all settings in the system.

From Ocularis ES 7.0 and onwards, you can create roles that have some or most rights of a system administrator. This may, for example, be relevant if your organization wants to separate between people who can administrate a subset of the system and people who can administer the entire system. The feature allows you to provide differentiated administrator permissions to access, edit or change a large variety of system functions, for example, the right to edit the settings for servers or cameras in your system. You can also reflect the same limitations in the user interface of the Management Client for each role by associating the role with a Management Client profile that has removed the corresponding system functions from the user interface. See About Management Client profiles (on page 78) for information.

To give a role such differentiated administrator rights, the person with the default full administrator role must set up the role under **Security > Roles > Info tab > Add new**. When you set up the new role, you can then associate the role with your own profiles must similarly to when you set up any other role in the system or use the system's default profiles. For more information, see Add and manage a role (on page 104).

Once you have specified what profiles you want to associate the role with, go to the **Overall Security** tab to specify the rights of the role.

The rights you can set for a role are different between Ocularis ES and Ocularis LS. While you can give all available rights to a role in Ocularis ES, you can only set non-administrator rights in Ocularis LS.

Add and manage a role

1. Expand *Security* and right-click *Roles*.
2. Select *Add Role*. This opens the *Add Role* dialog box.
3. Type a name and description of the new role and Click *OK*.

4. The new role is added to the *Roles* list. By default, a new role does not have any users/groups associated with it, but it does have a number of default profiles associated.
5. You can now assign users/groups to the role, and specify which of the system's features they can access.

Copy, rename or delete a role

Copy a role

If you have a role with complicated settings and/or rights and need a similar or almost similar role, it might be easier to copy the already existing role and make minor adjustments to the copy than to creating a new role from scratch.

1. Expand *Security*, click *Roles*, right-click the relevant role and select *Copy Role*.
2. In the dialog box that opens, give the copied role a new unique name and description.
3. Click *OK*.

Rename a role

If you rename a role, this does not change the name of the view group based upon the role.

1. Expand *Security*, and right-click *Roles*.
2. Right-click required role and select *Rename Role*.
3. In the dialog box that opens, change the name of the role.
4. Click *OK*.

Delete a role

1. Expand *Security*, and click *Roles*.
2. Right-click the unwanted role and select *Delete Role*.
3. Click *Yes*.

Important: If you delete a role, this does not delete the view group based upon the role.

Assign/remove users and groups to/from roles

To assign or remove Windows users or groups or basic users to/from a role:

1. Expand *Security* and select *Roles*. Then select the required role in the **Overview** pane:
2. In the **Properties** pane, select the *Users and Groups* tab at the bottom.
3. Click *Add*, select between **Windows user** or **Basic user**.

Assign Windows users and groups to a role

1. Select **Windows user**. This opens the *Select Users, Computers and Groups* dialog box:
2. Verify that the required object type is specified. If, for example, you need to add a computer, click *Object Types* and mark *Computer*. Also verify that the required domain is specified in the *From this location* field. If not, click *Locations* to browse for the required domain.
3. In the *Enter the object names to select* box, type the relevant user names, initials, or other types of identifier which Active Directory can recognize. Use the **Check Names** feature to verify that Active Directory recognizes the names or initials you have typed. Alternatively, use the **"Advanced..."** function to search for users or groups.
4. Click *OK*. The selected users/groups are now added to the *Users and Groups* tab's list of users who you have assigned the selected role. You can add more users and groups by entering multiple names separated by a semicolon (;).

Assign basic users to a role

1. Select **Basic User**. This opens the **Select Basic Users to add to Role** dialog box:
2. Select the basic user(s) that you want to assign to this role.
3. Optional: Click **New** to create a new basic user.
4. Click **OK**. The selected basic user(s) are now added to the *Users and Groups* tab's list of basic users who you have assigned the selected role.

Remove users and groups from a role

1. On the *Users and Groups* tab, select the user or group you want to remove and click **Remove** in the lower part of the tab. You can select more than one user or group, or a combination of groups and individual users, if you need to.
2. Confirm that you want to remove the selected user(s) or and group(s). Click **Yes**.

A user may also have roles through group memberships. When that is the case, you cannot remove the individual user from the role. Group members may also hold roles as individuals. To find out which roles users, groups, or individual group members have, use the **View Effective Roles** function.

View effective roles

With the Effective Roles feature, you can view all roles of a selected user or group. This is practical if you are using groups and it is the only way of viewing which roles a specific user is a member of.

1. Open the *Effective Roles* window by expanding *Security*, then right-clicking *Roles >Effective Roles*.
2. In the *Effective Roles* window's *User name* field, type the user name of the relevant user or use the "... " browse button.
3. If you typed the user name directly into the *User name*, click **Refresh** in the lower part of the window to display the roles of the user. If you used Active Directory to browse for the user, the user's roles are displayed automatically.

Roles settings

INFO TAB (ROLES)

On the **Info** tab of a role, you can set the following:

Name	Description
Name	Type a name for the role.
Description	Type a description for the role.
Management Client profile	Select a Management Client profile to associate with the role. You cannot apply this to the default Administrators role.
Default time profile	Select a default time profile to associate with the role. You cannot apply this to the default Administrators role.
Login authorization required	Select the check box to associate login authorization with the role. It means that Ocularis Client or the Management Client asks for a second authorization, typically by a superuser or manager, when the user logs in. To enable administrators to authorize users, configure the management server's Authorize Users right on the Overall Security tab. You cannot apply this to the default Administrators role.

USER AND GROUPS TAB (ROLES)

The term *users* primarily refers to users who connect to the surveillance system through the clients. You can configure such users in two ways:

- As **basic users**, authenticated by a user name/password combination.
- As **Windows users**, authenticated based on their Windows login

Windows Users

You add Windows Users through the use of Active Directory. Active Directory (AD) is a directory service implemented by Microsoft for Windows domain networks. It is included in most Windows Server operating systems. It identifies resources on a network in order for users or applications to access them. Active Directory uses the concepts of users and groups.

Users are Active Directory objects representing individuals with a user account. Example:



Groups are Active Directory objects with several users. In this example, the Management Group has three users:



Groups can contain any number of users. By adding a group to the system, you add all of its members in one go. Once you have added the group to the system, any changes made to the group in Active Directory, such as new members you add or old members you remove at a later stage, are immediately reflected in the system. Note that a user can be a member of more than one group at a time.

You can use Active Directory to add existing user and group information to the system with some benefits:

- Users and groups are specified centrally in Active Directory so you do not have to create user accounts from scratch.
- You do not have to configure any authentication of users on the system as Active Directory handles authentication.

Before you can add users and groups through the Active Directory service, you must have a server with Active Directory installed on your network.

Basic users

If your system does not have access to Active Directory, create a basic user instead. For information about how to set up basic users, see Create basic user (see "Create basic users" on page 121).

OVERALL SECURITY TAB (ROLES)

On the **Overall Security** tab, you set up overall rights for roles. For every component available in your system, decide whether to **Allow** or **Deny** users with the role the rights to access and use different areas on the relevant component.

The overall security settings only apply to the current site.

You can associate a user with more than one role. If you select **Deny** on a security setting for one role and **Allow** for another, the **Deny** right permission overrules the **Allow** right permission.

The **Overall Security** tab is available in both Ocularis ES and Ocularis LS, but the tab gives you the possibility to change more functionality in Ocularis ES than in Ocularis LS. This is because you can set up differentiated administrator rights in Ocularis ES, while such rights are not available in Ocularis LS.

In the following, the descriptions show what happens on each individual right for the different system components if you select **Allow** for the relevant role. If you use Ocularis LS, you can see which settings are not available to you under each system component.

For every system component or functionality, the full system administrator can use the **Allow** or **Deny** check boxes to set up security permissions for the role. Any security permissions you set up here is set up for the whole system component or functionality. So if, for example, you select the **Deny** check box on **Cameras**, all cameras added to the system are unavailable for the role. In contrast, if you select the **Allow** check box instead, the role can see all added cameras to the system. The result of selecting **Allow** or **Deny** on your cameras is that the camera settings on the **Device** tab then inherit your selections on the **Overall Security** tab so that either all cameras are available or unavailable to the particular role. If you want to set individual security permissions for individual cameras or similar device channels, you can then only set these individual permissions on the tab of the relevant system component or functionality if you have turned off any overall settings for the system component or functionality on the **Overall Security** tab.

If you switch your license from Ocularis ES to Ocularis LS, you can only do this if you have not set any security rights for the role for functionality that is not available in Ocularis LS. Therefore, to complete such a switch, make sure that you remove all security rights that are available to Ocularis ES only.

Management Server

Security right	Description	Ocularis LS
Full control	Enables the right to manage all security entries on this part of the system.	
Read	<p>Enables read access to general data on the Management Server which the individual object security does not handle:</p> <ul style="list-style-type: none"> ▶ Logging in with the Management Client ▶ List of current tasks ▶ Server Logs <p>It also enables access to the following features:</p> <ul style="list-style-type: none"> ▶ Remote Connect Services ▶ Management Client Profiles ▶ NetMatrix ▶ Time Profiles ▶ Registered Servers and Service Registration API ▶ Ocularis CS Servers 	Not available

Security right	Description	Ocularis LS
Edit	<p>Enables write access to general data on the server which the individual object security does not handle:</p> <ul style="list-style-type: none"> ▶ Options ▶ License Management <p>It also enables users to create, delete and edit the following features:</p> <ul style="list-style-type: none"> ▶ Remote Connect Services ▶ Device groups ▶ Management Client Profiles ▶ NetMatrix ▶ Time Profiles ▶ Registered Servers ▶ Ocularis CS Servers <hr/> <p>Enables the right to configure local IP ranges when configuring the network on the recording server.</p>	Not available
System Monitor	Enables the right to view the data of the System Monitor.	
Status API	Enables the right to perform queries on the Status API located on the recording server. This means that the role with this right enabled, has access to read the status of the items located on the recording server.	Not available
Manage Federated site hierarchy	<p>Enables the right to add and detach the current site to other sites in a Federated Architecture federated site hierarchy.</p> <hr/> <p>If you set this permission to allowed on the child site only, the user can still detach the site from the parent site.</p>	
Backup Configuration	Enables the right to create backups of the system configuration using the system's backup/restore functionality.	
Manage security	Enables the right to manage permissions for the Management Server. It also enables users to manage roles, to add or remove members of roles and to create and delete basic users.	
Authorize users	Enables the right to authorize users when they are asked for a second login in Management Client. You define if a role requires login authorization on the Info tab.	Not available

Recording Servers

The following settings are only available in Ocularis ES.

Security right	Description
Full control	Enables the right to manage all security entries on this part of the system.
Edit	Enables the right to edit properties on the recording servers, except for network configuration settings that require Edit right on the management server.

Delete	Enables the right to delete recording servers. To do this, you must also give the user delete permissions on: <ul style="list-style-type: none"> ▶ Hardware security group if you have added hardware to the recording server.
Manage hardware	Enables the right to add hardware on recording servers.
Manage storage	Enables the right to administrate storage containers on recording server, that is to create, delete, move and empty storage containers.
Authorize recording server	Enables the right to authorize new recording servers.
Manage security	Enables the right to manage security permissions for recording servers.

Failover Servers

The following settings are only available in Ocularis ES.

Security right	Description
Full control	Enables the right to manage all security entries on this part of the system.
Read	Enables the right to see and access failover servers in the Management Client.
Edit	Enables the right to edit properties on failover servers in the Management Client.
Manage security	Enables the right to manage security permissions for the failover servers.

Hardware

The following settings are only available in Ocularis ES.

Security right	Description
Full control	Enables the right to manage all security entries on this part of the system.
Edit	Enables the right to edit properties on hardware.
Delete	Enables the right to delete hardware.
Manage security	Enables the right to manage security permissions for the hardware.

Cameras

Security right	Description	Ocularis LS
Full control	Enables the right to manage all security entries on this part of the system.	
Read	Enables the right to view camera devices in the clients.	
Edit	Enables the right to edit properties for cameras in the Management Client. It also enables users to enable or disable a camera.	Not available
View Live	Enables the right to view live video from cameras in the clients.	

Security right	Description	Ocularis LS
Playback	Enables the right to play back recorded video from cameras in the clients.	
Retrieve remote recordings	Enables the right to retrieve edge recordings from cameras or recordings from cameras on remote sites.	
Read sequences	Enables the right to read the sequence information related to, for example, the Sequence explorer in the clients.	
Smart search	Enables the right to use the Smart search function in the clients.	
Export	Enables the right to export recordings from the clients.	
Start manual recording	Enables the right to start manual recording of video in the clients.	
Stop manual recording	Enables the right to stop manual recording of video in the clients.	
AUX commands	Enables the right to use auxiliary (AUX) commands on the camera from the clients. AUX commands offer users the control of for example, wipers on a camera connected via a video server. Camera-associated devices connected via auxiliary connections are controlled from the client.	
PTZ control	Enables the right to use the pan, tilt and zoom features of PTZ cameras.	
Activate PTZ preset	Enables the right to move PTZ cameras to preset positions.	
Delete recordings	Enables the right to delete stored video recordings from the system.	Not available
Manage security	Enables the right to manage security permissions for the camera.	Not available

Microphones

Security right	Description	Ocularis LS
Full control	Enables the right to manage all security entries on this part of the system.	
Read	Enables the right to view microphone devices in the clients.	
Edit	Enables the right to edit microphone properties in the Management Client. It also allows users to enable or disable microphones.	Not available
Listen	Enables the right to listen to live audio from microphones in the clients.	
Playback	Enables the right to play back recorded audio from microphones in the clients.	
Retrieve remote recordings	Enables the right to retrieve edge recordings from microphones or recordings from microphones on remote sites.	
Read sequences	Enables the right to read the sequence information related to, for example, the Sequence explorer in the clients.	
Export	Enables the right to export recordings from the clients.	

Security right	Description	Ocularis LS
Start manual recording	Enables the right to start manual recording of audio in the clients.	
Stop manual recording	Enables the right to stop manual recording of audio in the clients.	
Delete recordings	Enables the right to delete stored recordings from the system.	Not available
Manage security	Enables the right to manage security permissions for microphones.	Not available

Speakers

Security right	Description	Ocularis LS
Full control	Enables the right to manage all security entries on this part of the system.	
Read	Enables the right to view speaker devices in the clients.	
Edit	Enables the right to edit properties for speakers in the Management Client. It also allows users to enable or disable speakers.	Not available
Listen	Enables the right to listen to live audio from speakers in the clients.	
Speak	Enables the right to speak through the speakers in the clients.	
Playback	Enables the right to play back recorded audio from speakers in the clients.	
Retrieve remote recordings	Enables the right to retrieve edge recordings from speakers or recordings from speakers on remote sites.	
Read sequences	Enables the right to use the Sequences feature while browsing recorded audio from speakers in the clients.	
Export	Enables the right to export recorded audio from speakers in the clients.	
Start manual recording	Enables the right to start manual recording of audio in the clients.	
Stop manual recording	Enables the right to stop manual recording of audio in the clients.	
Delete recordings	Enables the right to delete stored recordings from the system.	Not available
Manage security	Enables the right to manage security permissions for speakers.	Not available

Metadata

Security right	Description	Ocularis LS
Full control	Enables the right to manage all security entries on this part of the system.	
Read	Enables the right to receive metadata in the clients.	

Security right	Description	Ocularis LS
Edit	Enables the right to edit metadata properties in the Management Client. It also allows users to enable or disable metadata devices.	Not available
Live	Enables the right to receive live metadata from cameras in the clients.	
Playback	Enables the right to play back recorded data from metadata devices in the clients.	
Retrieve remote recordings	Enables the right to retrieve edge recordings from metadata devices or recordings from metadata devices on remote sites.	
Read sequences	Enables the right to read the sequence information related to, for example, the Sequence explorer in the clients.	
Export	Enables the right to export recordings in the clients.	
Start manual recording	Enables the right to start manual recording of metadata in the clients.	
Stop manual recording	Enables the right to stop manual recording of metadata in the clients.	
Delete recordings	Enables the right to delete stored recordings from the system.	Not available
Manage security	Enables the right to manage security permissions for metadata.	Not available

Input

Security right	Description	Ocularis LS
Full control	Enables the right to manage all security entries on this part of the system.	Not available
Read	Enables the right to view input devices in the clients.	
Edit	Enables the right to edit properties for input devices in the Management Client. It also enables users to enable or disable an input device.	Not available
Manage security	Enables the right to manage security permissions for input devices.	Not available

Output

Security right	Description	Ocularis LS
Full control	Enables the right to manage all security entries on this part of the system.	
Read	Enables the right to view output devices in the clients.	
Edit	Enables the right to edit properties for output devices in the Management Client. It also enables users to enable or disable an output device.	Not available
Activate	Enables the right to activate outputs in the clients.	

Security right	Description	Ocularis LS
Manage security	Enables the right to manage security permissions for output devices.	Not available

View Groups

Security right	Description	Ocularis LS
Full control	Enables the right to manage all security entries on this part of the system.	
Read	Enables the right to view the View Groups created in the Management Client in the clients.	
Edit	Enables the right to edit properties on the View groups in the Management Client.	Not available
Delete	Enables the right to delete View Groups in the Management Client.	Not available
Operate	Enables the right to use View Groups created in the Management Client within the clients, that is to create subgroups and views.	
Manage security	Enables the right to manage security permissions for View Groups.	Not available
Create view group	Enables the right to create new View Groups in the Management Client.	Not available

User-defined Events

Security right	Description	Ocularis LS
Full control	Enables the right to manage all security entries on this part of the system.	
Read	Enables the right to view user-defined events in the Management Client and the clients.	
Edit	Enables the right to edit properties on user-defined events in the Management Client.	Not available
Delete	Enables the right to delete user-defined events in the Management Client.	Not available
Trigger	Enables the right to trigger user-defined events in the clients.	
Manage security	Enables the right to manage security permissions for user-defined events.	Not available
Create user-defined event	Enables the right to create new user-defined events in the Management Client.	Not available

NetMatrix

Security right	Description	Ocularis LS
Full control	Enables the right to manage all security entries on this part of the system.	Not available
Read	Enables the right to select and send video to the NetMatrix recipient from the clients.	
Edit	Enables the right to edit properties for the NetMatrix recipient.	Not available
Delete	Enables the right to delete NetMatrix users.	Not available
Manage security	Enables the right to manage security permissions for all NetMatrix users.	Not available
Create NetMatrix	Enables the right to create new NetMatrix users.	Not available

Rules

The following settings are only available in Ocularis ES.

Security right	Description
Full control	Enables the right to manage all security entries on this part of the system.
Read	Enables the right to view existing rules in the Management Client.
Edit	Enables the right to edit properties for rules and to define rule behavior in the Management Client. It also requires that the user has read permissions on all devices that are impacted by the rule.
Delete	Enables the right to delete rules from the Management Client. It also requires that the user has read permissions on all devices that are impacted by the rule.
Manage security	Enables the right to manage security permissions for all rules.
Create rule	Enables the right to create new rules. It also requires that the user has read permissions on all devices that are impacted by the rule.

Sites

The following settings are only available in Ocularis ES.

Security right	Description
Full control	Enables the right to manage all security entries on this part of the system.
Read	Enables the right to view other sites in the Management Client. Connected sites are connected via OnSSI Federated Architecture.
Edit	Enables the right to edit properties on other sites in the Management Client. Connected sites are connected via OnSSI Federated Architecture.

Security right	Description
Manage security	Enables the right to manage security permissions all sites.

DEVICE TAB (ROLES)

The *Device* tab lets you specify which features users/groups with the selected role can use for each device (for example, a camera) or device group in Ocularis Client.

Remember to repeat for each device. You can also select a device group, and specify role rights for all the devices in the group in one go.

You can still select or clear such square-filled check boxes, but note that your choice in that case applies for *all* devices within the device group. Alternatively, select the individual devices in the device group to verify exactly which devices the relevant right applies for.

Camera-related rights

Specify the following rights for camera devices:

Name	Description
Read	The selected camera(s) will be visible in the clients.
View live	Allows live viewing of video from the selected camera(s) in the clients. For Ocularis Client, it requires that the role has been granted the right to view the clients' <i>Live</i> tab. This right is granted as part of the application rights. Specify the time profile or leave the default value.
Playback > Within time profile	Allows playback of recorded video from the selected camera(s) in the clients. Specify the time profile or leave the default value.
Playback > Limit playback to	Allows playback of recorded video from the selected camera(s) in the clients. Specify a playback limit or apply no restrictions.
Read sequences	Allows reading the sequence information related to, for example, the Sequence explorer in the clients.
Smart search	Allows the user to use the Smart search function in the clients.
Export	Allows the user to export recordings from the clients.
Start manual recording	Allows starting manual recording of video from the selected camera(s) in the clients.
Stop manual recording	Allows stopping manual recording of video from the selected camera(s) in the clients.
AUX commands	Allows the use of auxiliary commands from the clients.

Microphone-related rights

Specify the following rights for microphone devices:

Name	Description
Read	The selected microphone(s) will be visible in the clients.

Name	Description
Live > Listen	Allows listening to live audio from the selected microphones(s) in the clients. For Ocularis Client, it requires that the role has been granted the right to view the clients' <i>Live</i> tab. This right is granted as part of the application rights. Specify the time profile or leave the default value.
Playback > Within time profile	Allows playback of recorded audio from the selected microphone(s) in the clients. Specify the time profile or leave the default value.
Playback > Limit playback to	Allows playback of recorded audio from the selected microphone(s) in the clients. Specify a playback limit or apply no restrictions.
Read sequences	Allows reading the sequence information related to, for example, the Sequence explorer in the clients.
Export	Allows the user to export recordings from the clients.
Start manual recording	Allows starting manual recording of audio from the selected microphone(s) in the clients.
Stop manual recording	Allows stopping manual recording of audio from the selected microphone(s) in the clients.

Speaker-related rights

Specify the following rights for speaker devices:

Name	Description
Read	The selected speaker(s) is visible in the clients.
Live > Listen	Allows listening to live audio from the selected speaker(s) in the clients. For Ocularis Client, it requires that the role has been granted the right to view the clients' <i>Live</i> tab. This right is granted as part of the application rights. Specify the time profile or leave the default value.
Playback > Within time profile	Allows playback of recorded audio from the selected speaker(s) in the clients. Specify the time profile or leave the default value.
Playback > Limit playback to	Allows playback of recorded audio from the selected speaker(s) in the clients. Specify a playback limit or apply no restrictions.
Read sequences	Allows reading the sequence information related to, for example, the Sequence explorer in the clients.
Export	Allows the user to export recordings from the clients.
Start manual recording	Allows starting manual recording of audio from the selected speaker(s) in the clients.
Stop manual recording	Allows stopping manual recording of audio from the selected speaker(s) in the clients.

Metadata-related rights

Specify the following rights for metadata devices:

Name	Description
Read	Enables the right to see metadata devices and retrieve data from them in the clients.
Edit	Enables the right to edit metadata properties. .
View Live	Enables the right to view metadata from cameras in the clients. For Ocularis Client, it requires that the role has been granted the right to view the clients' <i>Live</i> tab. This right is granted as part of the application rights.
Playback	Enables the right to play back recorded data from metadata devices in the clients.
Read sequences	Enables the right to use the Sequences feature while browsing recorded data from metadata devices in the clients.
Export	Enables the right to export recorded audio from metadata devices in the clients.
Start manual recording	Enables the right to start manual recording of metadata in the clients.
Stop manual recording	Enables the right to stop manual recording of metadata in the clients.

Input-related rights

Specify the following rights for input devices:

Name	Description
Read	The selected input(s) will be visible in the clients as well as in NetCentral, an add-on product for providing complete overview of surveillance system status and alarms.

Output-related rights

Specify the following rights for output devices:

Name	Description
Read	The selected output(s) will be visible in the clients. If visible, the output will be selectable on a list in the clients.
Activate	The selected output(s) can be activated from the Management Client and the clients. Specify the time profile or leave the default value.

PTZ TAB (ROLES)

You set up rights for pan-tilt-zoom (PTZ) cameras on the **PTZ** tab. You can specify the features users/groups can use in the clients. You can select individual PTZ cameras or device groups containing PTZ cameras.

Specify the following rights for PTZ:

Name	Description
<i>PTZ Control</i>	Determines if the selected role can use PTZ features on the selected camera. Specify the time profile or leave the default value.
<i>Activate PTZ preset</i>	Determines if the selected role can move the selected PTZ cameras to preset positions. Specify the time profile or leave the default value.
<i>PTZ Priority</i>	<p>Determines the priority of PTZ cameras. When several users on a surveillance system want to control the same PTZ camera at the same time, conflicts may occur.</p> <p>You can avoid such a situation by specifying a priority for use of the selected PTZ camera(s) by users/groups with the selected role. Specify a priority from 1 to 32,000, where 1 is the lowest priority. The default priority is 3,000. The role with the highest priority number is the one who can control the PTZ camera(s).</p>

SPEECH TAB (ROLES)

Relevant only if you use speakers on your system. Specify the following rights for speakers:

Name	Description
<i>Speak</i>	Determine if users should be allowed to talk through the selected speaker(s). Specify the time profile or leave the default value.
<i>Speak priority</i>	<p>When several client users want to talk through the same speaker at the same time, conflicts may occur.</p> <p>Solve the problem by specifying a priority for use of the selected speaker(s) by users/groups with the selected role. Specify a priority from <i>Very low</i> to <i>Very high</i>. The role with the highest priority is allowed use the speaker before other roles.</p> <p>Should two users with the same role want to speak at the same time, the first come, first served-principle applies.</p>

REMOTE RECORDINGS TAB (ROLES)

Specify the following rights for remote recordings:

Name	Description
<i>Retrieve remote recordings</i>	Determines if users/groups with the selected role can retrieve remote recordings.

EXTERNAL EVENT TAB (ROLES)

Specify the following external event rights:

Name	Description
<i>Read</i>	Allows users to search for and view external system events in Ocularis Client.
<i>Edit</i>	Allows users to edit external system events in Ocularis Client.

Name	Description
Delete	Allows users to delete external system events in Ocularis Client.
Trigger	Allows users to trigger external system events in Ocularis Client.

VIEW GROUP TAB (ROLES)

On the View Group tab, you specify which view groups the users and user groups with the selected role can use in the clients.

Specify the following rights for view groups:

Name	Description
Read	Determine if the selected role can see the selected view group (and any views contained in the view group) in the clients.
Edit	Determine if the selected role can make changes to the selected view group (and any views contained in the view group) in the clients.
Delete	Determine if the selected role can delete the selected view group (and any views contained in the view group) in the clients.
Operate	Determine if the selected role can create subgroups and views in the clients.

SERVERS TAB (ROLES)

Specifying role rights on the *Servers* tab is only relevant if you have integrated Ocularis CS servers into your system or your system works in a OnSSI Federated Architecture setup.

See About Ocularis CS servers (see "About Ocularis CS servers" on page 151) or About OnSSI Federated Architecture (on page 142) for more information.

NETMATRIX TAB (ROLES)

If you have configured NetMatrix recipients on your system, you may configure NetMatrix role rights. From a client, you can send video to selected NetMatrix recipients. Select the users who can receive this on the NetMatrix tab.

The following rights are available:

Name	Description
Read	Determine if users and groups with the selected role can select and send video to the NetMatrix recipient from the clients.

Basic users

About basic users

When you add a basic user to your system, you create a dedicated surveillance system user account with basic user name and password authentication for the individual user. This is in contrast to the Windows user, added through Active Directory. See the User and Groups tab (see "User and Groups tab (roles)" on page 107) under **Roles** for more information.

Create basic users

To create a basic user on your system:

1. Expand **Security > Basic Users**.
2. In the Basic Users pane, right-click and select **Create Basic User**.
3. Specify a user name and a password, and repeat it to be sure you have specified it correctly.
4. Click **OK** to create the basic user.

System dashboard

About system dashboard

On System Dashboard, find the following functionality:

Name	Description
System Monitor	View and print detailed system reports on servers, devices and cameras.
Current Task	Get an overview of tasks under a selected recording server.
Configuration Report	Decide what to include in your system configuration reports before printing.

About system monitor

System Monitor allows you to view system information and create reports regarding:

Management server	Shows data on your management server
Recording server(s)	Shows data on any number of recording servers in your setup. You can view these per: Disk Storage Network Camera
Failover recording servers	Shows data on any number of failover recording servers in your setup.
Additional servers	Shows data on log server.
Cameras	Shows data on any camera in any camera group in your setup.

Each of these elements are a clickable, expandable area and most of these include sub-areas. Each sub-area represents a server. When clicked, they provide relevant dynamic data on this server.

The *Cameras* bar contains a list of camera groups to select from. Once you select a group, select a specific camera and see dynamic data for it. All servers display CPU usage and available memory information. Recording servers also display connection status information. Within each view, find a *History* link. Click it to view historic data and reports (to view reports on a camera, click the name of the camera). For each historic report, you can view data for the last 24 hours, 7 days or 30 days. To save and/or print reports, click the *Send to PDF* icon. Use the < and home icons to navigate System Monitor.

Important: If you access system monitor from a server operating system, you may experience a message regarding *Internet Explorer Enhanced Security Configuration*. Follow instructions in the message to add the System Monitor page to the *Trusted sites zone* before proceeding.

Restart Data Collector Server service

Your system automatically installs the Data Collector Server service on the same computers as the management, recording, and log server(s).

Normally, the Data Collector Server service requires no maintenance, but if the service **does** stop, no live feed is sent to the System Monitor (clearly indicated in System Monitor by error texts). On the computer on which you have installed the Data Collector Server service, do the following:

1. In Windows' *Start* menu, select *Control Panel*, and then:
 - If using *Category* view, find the *System and Security* category and click *Administrative Tools*.
 - If using *Small icons* or *Large icons*, click *Administrative Tools*.
2. Double-click **Services**.
3. Locate the **OnSSI Data Collector Server**. Right-click it and select **Start** to restart the service.

About current tasks

Current Tasks show an overview of tasks under a selected recording server, their begin time, estimated end time and progress. All information shown in **Current Tasks** are snapshots. You can refresh these by clicking on the **Refresh** button in the lower right corner of the **Properties** pane.

About configuration reports

When you create PDF configuration reports, you can include any possible elements of your system in the report. You can, for example, include licenses, device configuration, alarm configuration, and much more. You can also customize your font and page setup and include a customized front page.

Add a configuration report

1. Expand *System Dashboard* and click *Configuration Reports*. This brings up the report configuration page.
2. Select the elements that you want to include in your report.
3. Optional: Click *Front Page* to customize your front page. In the window that appears, fill in the needed info. Select *Front page* as an element to include in your report, otherwise the front page you customize is not included in your report.
4. Click *Formatting* to customize your font, page size and margins. In the window that appears, select the wanted settings.
5. When you are ready to export, click *Export* and select a name and save location for your report.

Configure report details

The following is available when setting up reports:

Name	Description
Select All	Selects all elements in the list.
Clear All	Clears all elements in the list.
Front Page	Customize the front page of the report.
Formatting	Format the report.
Export	Select a save location for the report and create a PDF.

Server logs

About logs

You can view and export contents from different logs related to the system. The purpose of the logs is to document activity, events, actions and errors in the system, for later analysis or documentation.

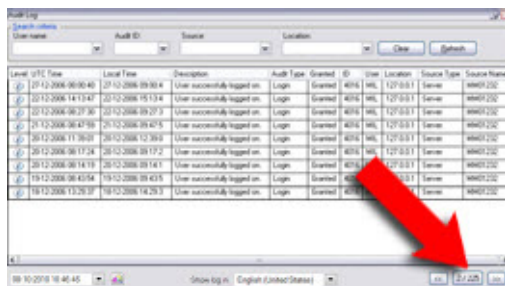
The logs have different purposes:

Name	Description
System log	Logs system-related information.
Audit log	Logs user activity.
Rule log	Logs rules in which users have specified the Make new log entry action.

Your system has a number of default settings related to the different logs. To change the settings, see Server Logs tab (see "Server Logs tab (options)" on page 128) under Options.

You can view logs in a number of different languages and export logs as tab delimited text (.txt) files.

If a log contains more than one page of information, you can navigate between the log pages by clicking the buttons in the bottom right corner of the log pane:



In the lower left corner, jump to a specific date and time in the log:



Search logs

To search a log, use *Search criteria* in the top part of the log pane:


1. Specify your search criteria from the lists.
2. Click *Refresh* to make the log page reflect your search criteria. To clear your search criteria, and return to viewing all of the log's content, click **Clear**.

You can double-click any row to have all details presented in a **Log Details** window. In this way you can also read the log entries that contain more text than can be displayed in a single line.

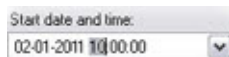
Export logs

You can export logs as tab delimited text (.txt) files. You can customize the log content by specifying which log, log elements, and time range to include in the export. For example, you can specify to include only the System Log error-related log entries from between January 2nd 2011 08:00:00 and January 4th 2011 07:59:59 in your export.

To export a log:

1. In the *Export Log* window's *Filename* field, specify a name for the exported log file.
By default, exported log files are saved in your *My Documents* folder. However, you can specify a different location by clicking the browse button  next to the field.
2. Any criteria you have selected to target the content of the exported log is listed in the *Filters* field. You cannot edit this field. If you need to change your criteria, close the window, and repeat steps 1-2.
3. Specify the time period you want the export to cover. Specify the *Start date and time* and *End date and time* fields respectively. You can select the date by clicking the arrow:

To specify an exact time, overwrite the required time elements (hours:minutes:seconds) with the needed values. In this example, the hours element is being overwritten:



4. Click *Export* to export the log content.

Change log language




1. At the bottom part of the log pane, in the *Show log in* drop down-box, select the wanted language.



2. The log is displayed in the selected language. Next time you open the log, it is reset to the default language.

System log properties




Each row in a log represents a log entry. A log entry contains a number of information fields:

Name	Description
Level	Displays an icon that indicates the level of the log entry:  - indicates info  - indicates warning  - indicates error 'blank' - indicates an undefined entry.
UTC Time	Timestamped in coordinated universal time (UTC).
Local Time	Timestamped in the local time of your system's server.

Name	Description
ID	The identification number for the logged incident.
Source Type	The type of equipment on which the logged incident occurred, for example, server or device.
Source Name	Management server, the name of the recording server or device on which the logged incident occurred.
Event Type	The type of event represented by the logged incident.
Description	Shows a description of the logged incident.




Audit log properties

Each row in a log represents a log entry. A log entry contains a number of information fields:

Name	Description
Level	Displays an icon that indicates the level of the log entry:  - indicates info  - indicates warning  - indicates error 'blank' - indicates an undefined entry.
UTC Time	Timestamped in coordinated universal time (UTC).
Local Time	Timestamped in the local time of your system's server.
ID	The identification number for the logged incident.
User	The user name of the remote user causing the logged incident.
User Location	The IP address or host name of the computer from which the remote user caused the logged incident.
Permission	The information about whether the remote user action was allowed (granted) or not.
Category	The type of logged incident.
Resource Type	The type of equipment on which the logged incident occurred, for example, server or device.
Resource Name	Management server, or the name of the recording server or device on which the logged incident occurred.
Resource Host	The name of the recording server that hosts a device or a storage on which the logged incident occurred. The name of the management server that hosts the recording server or the management server on which the logged incident occurred.
Description	Shows a description of the logged incident.

Rule log properties

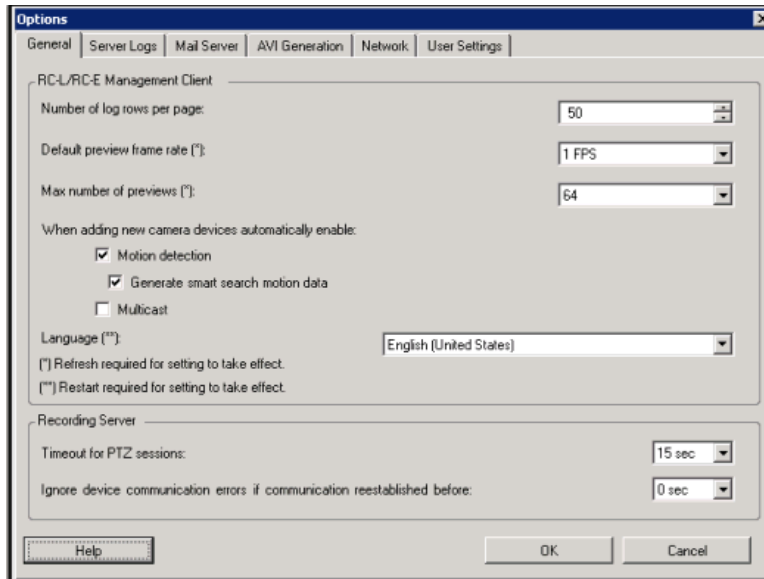
Each row in a log represents a log entry. A log entry contains a number of information fields:

Name	Description
Level	Displays an icon that indicates the level of the log entry:  - indicates info  - indicates warning  - indicates error 'blank' - indicates an undefined entry.
UTC Time	Timestamped in coordinated universal time (UTC).
Local Time	Timestamped in the local time of your system's server.
ID	The identification number for the logged incident.
Service Name	The name of the service on which the logged incident occurred.
Rule Name	The name of the rule triggering the log entry.
Source Type	The type of equipment on which the logged incident occurred, for example, server or device.
Source Name	Management server, the name of the recording server or device on which the logged incident occurred.
Event Type	The type of event represented by the logged incident.
Generator Type	The type of equipment on which the logged incident was triggered. Log entries are administrator-defined and relate to incidents in your system.
Generator Name	The name of the equipment on which the logged incident was generated.
Description	Shows a description of the logged incident.

Options dialog box

In the *Options* dialog box, you can specify a number of settings related to the general appearance and functionality of the system.

To access the dialog box, select *Tools > Options*.



The *Options* dialog box features the following tabs:

- General tab (see "General tab (options)" on page 127)
- Server Logs tab (see "Server Logs tab (options)" on page 128)
- Mail Server tab (see "Mail Server tab (options)" on page 129)
- AVI Generation tab (see "AVI Generation tab (options)" on page 129)
- Network tab (see "Network tab (options)" on page 130)
- User Settings tab (see "User Settings tab (options)" on page 130)

General tab (options)

On the General tab, you can specify general settings for the Management Client and the recording server.

Management Client

Name	Description
Number of log rows per page	Select how many rows a single log page can contain. The default value is 50 rows. If a log contains more rows, it displays the next rows on the following pages.
Default preview frame rate	Select frame rate for the thumbnail camera images displayed in the Preview pane. Default is 1 frame per second. Select <i>Action > Refresh</i> from the menu for the change to take effect. Note that a high frame rate in combination with a large number of thumbnail images in the Preview pane slows down the computer that runs the Management Client. You can limit the number of thumbnail images with the <i>Max number of previews</i> setting.

Name	Description
Max number of previews	<p>Select the maximum number of thumbnail images displayed in the Preview pane. Default is 64 thumbnail images.</p> <p>Select <i>Action > Refresh</i> from the menu for the change to take effect.</p> <p>Note that a large number of thumbnail images in combination with a high frame rate may slow the system down. You can limit the frame rate used for the thumbnail images with the <i>Default preview frame rate</i> setting.</p>
When adding new camera devices automatically enable: Motion detection	<p>Select the check box to enable motion detection on new cameras, when you add them to the system with the <i>Add Hardware</i> wizard.</p> <p>This setting does not affect motion detection settings on existing cameras.</p> <p>You enable and disable motion detection for a camera on the Motion tab for the camera device.</p>
When adding new camera devices automatically enable: Generate motion data for smart search	<p>Generation of motion data for smart search requires that motion detection is enabled for the camera.</p> <p>Select the check box to enable generation of smart search motion data on new cameras, when you add them to the system with the <i>Add Hardware</i> wizard.</p> <p>This setting does not affect motion detection settings on existing cameras.</p> <p>You enable and disable the generation of smart search motion data for a camera on the Motion tab for the camera device.</p>
When adding new camera devices automatically enable: Multicast	<p>Select the check box to enable multicast on new cameras when you add them with the <i>Add Hardware</i> wizard.</p> <p>This setting does not affect multicast settings on existing cameras.</p> <p>You enable and disable live multicasting for a camera on the Client tab for the camera device.</p>
Language	<p>Select the language of the Management Client.</p> <p>Restart the Management Client to use the new language.</p>

Recording server

Name	Description
Timeout for PTZ sessions	<p>Client users with the necessary user rights can manually interrupt the patrolling of PTZ cameras. Select how much time should pass before regular patrolling is resumed after a manual interruption. The setting applies for all PTZ cameras on your system.</p>
Ignore device communication errors if communication reestablished before	<p>Select for how long a communication error may exist before the system logs it as an error and triggers the Communication Error event.</p>

Server Logs tab (options)

On the *Server Logs* tab, you can specify settings for the system's management server logs.

See also About logs (on page 123) for more information.

Name	Description
Logs	<p>Select the log that you want to configure:</p> <ul style="list-style-type: none"> ▶ System Log ▶ Audit Log ▶ Rule Log
Settings	<p>Disable/enable the logs and specify the retention period and the maximum number of rows for each log.</p> <p>For System logs, specify the level of messages you want to log:</p> <ul style="list-style-type: none"> ▶ All - includes undefined messages ▶ Information, warnings and errors ▶ Warnings and errors ▶ Errors (default setting) <p>For Audit logs, enable user access logging if you want the system to log all recorder user actions. These are, for example, exports, activating outputs, viewing cameras live or in playback.</p> <p>Specify:</p> <ul style="list-style-type: none"> ▶ the length of a playback sequence. This means that as long as the user plays back within this period, the system only generates one log entry. When playing back outside the period, the system creates a new log entry. ▶ the number of records (frames) a user has seen before the system creates a log entry.

Mail Server tab (options)

On the *Mail Server* tab, you can specify the settings for your system's outgoing SMTP mail server. See also About notification profiles (on page 100).

Name	Description
Sender e-mail address	Type the e-mail address you want to appear as the sender of e-mail notifications for all notification profiles. Example: sender@organization.org.
Outgoing mail (SMTP) server name	Type the name of the SMTP mail server that sends e-mail notifications. Example: mailserver.organization.org.
Server requires login	Specify a user name and password for the users to log into the mail server.

AVI Generation tab (options)

On the *AVI Generation* tab, you can specify compression settings for the generation of AVI video clip files. The settings are required if you want to include AVI files in e-mail notifications sent by rule-triggered notification profiles.

See also Use rules to trigger email notifications (on page 101).

Name	Description
Compressor	Select the codec (compression/decompression technology) that you want to apply. To have more codecs available in the list, install them on the management server. Not all cameras support all codecs.
Compression quality	(Not available for all codecs). Use the slider to select the degree of compression (0-100) to be performed by the codec. 0 means no compression, generally resulting in high image quality and large file size. 100 means maximum compression, generally resulting in low image quality and small file size. If the slider is not available, the compression quality is determined entirely by the selected codec.
Keyframe every	(Not available for all codecs). If you want to use keyframes, select the check box and specify the required number of frames between keyframes. A keyframe is a single frame stored at specified intervals. The keyframe contains the entire view of the camera, whereas the following frames contain only the pixels that change. This helps greatly reduce the size of files. If the check box is not available, or not selected, every frame contains the entire view of the camera.
Data rate	(Not available for all codecs). If you want to use a particular data rate, select the check box and specify the number of kilobytes per second. The data rate specifies the size of the attached AVI file. If the check box is not available, or not selected, the data rate is determined by the selected codec.

Network tab (options)

On the *Network* tab, you can specify the IP addresses of the local clients, if the clients are to connect to the recording server via the Internet. The surveillance system then recognizes them as coming from the local network.

User Settings tab (options)

On the *User Settings* tab, you can specify user preference settings, for example, if a message should be shown when remote recording is enabled.

Failover configuration

Failover recording servers (regular and hot standby)

About failover recording servers

A failover recording server is an extra recording server which takes over from a normal recording server if this becomes unavailable. You can configure a failover recording server in two ways, as a **regular failover recording server** or as a **hot standby server**.

You install failover recording servers like regular recording servers. Once you have installed failover recording servers, they are visible in the Management Client. You should install all failover recording servers on separate computers. Make sure that you configure failover recording servers with the correct IP address/hostname of the management server and that you verify that the user account under which the Failover Server service runs has access to your system with administrator rights.

You can specify what type of failover support you want on device-level. For each device on a recording server, select full, live only or no failover support. This helps you prioritize your failover resources and, for example, only set up failover for video and not for audio, or only have failover on essential cameras, not on less important ones.

Regular failover servers

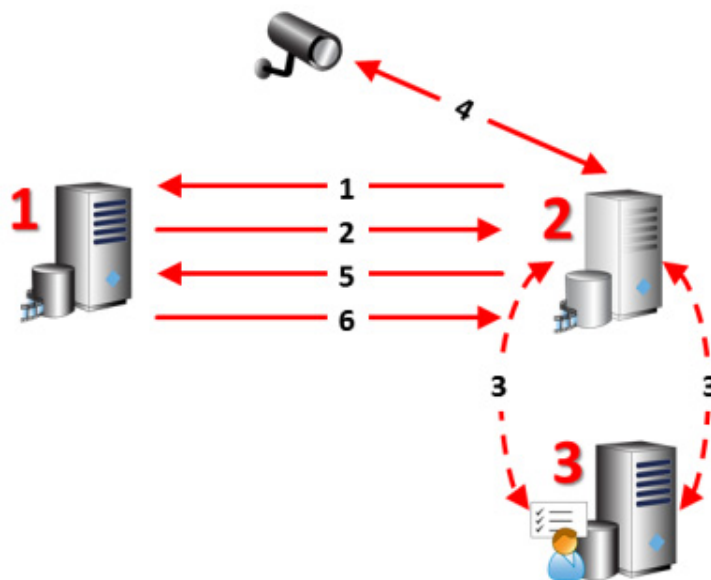
In a regular failover recording server setup, you can group a failover recording server with other failover recording servers in a failover group. The entire failover group is dedicated to taking over from any of several preselected recording servers, should one of these become unavailable.

A failover group can contain one or more regular failover recording servers. Grouping has a clear benefit: when you later specify which failover recording servers should take over from a recording server, you select a group of failover recording servers. If the selected group contains more than one failover recording server, this offers you the security of having more than one failover recording server ready to take over if a recording server becomes unavailable. You can create as many failover groups as needed group them as needed. A failover recording server can only be a member of one group at a time.

Failover recording servers in a failover group are ordered in sequence. This sequence determines in which order the failover recording servers should take over from a recording server. By default, this sequence reflects the order in which you have incorporated the failover recording servers have in the failover group: first in is first in sequence. You can change this if you need to.

Hot standby failover recording servers

In a hot standby recording server setup, you can dedicate a failover recording server to take over from **one** recording server only. Because of this, the system can keep this failover recording server in a "standby" mode which means that it already starts with the correct/current configuration of the recording server it is dedicated to and can take over faster than a regular failover recording server. As mentioned, you assign hot standby servers to one recording server only and cannot group it. You cannot select to use failover servers that are already part of a failover group as hot standby recording servers.

About failover steps

Involved **servers** (numbers in red):

1. Recording server
2. Failover recording server
3. Management server.

Failover steps for **Regular failover** setups:

1. To check whether it is running or not, a failover recording server has a non-stop TCP connection to a recording server.
2. This connection is interrupted.
3. The failover recording server requests the current configuration of the recording server from the management server. The management server sends the requested configuration, the failover recording server receives the configuration, starts up, and starts recording on behalf of the recording server.
4. The failover recording server and the relevant camera(s) exchange video data.
5. The failover recording server continually tries to re-establish connection to the recording server.
6. When the connection to the recording server is re-established, the failover recording server shuts down and the recording server fetches video data (if any) recorded during its down-time and the video data is merged back in to the recording server database.

Failover steps for **hot standby** setups:

1. To check whether it is running or not, a hot standby server has a non-stop TCP connection to its assigned recording server.
2. This connection is interrupted.
3. From the management server, the hot standby server already knows the current configuration of its assigned recording server and starts recording on its behalf.
4. The hot standby server and the relevant camera(s) exchange video data.
5. The hot standby server continually tries to re-establish connection to the recording server.
6. When the connection to the recording server is re-established and the hot standby server goes back to hot standby mode, the recording server fetches video data (if any) recorded during its down-time and the video data is merged back in to the recording server database.

About failover recording server functionality

- A failover recording server checks the state of relevant recording servers every single 0.5 seconds. If a recording server does not reply within 2 seconds, the recording server is considered unavailable and the failover recording server takes over.
- A regular failover recording server takes over for the recording server that has become unavailable after five seconds plus the time it takes for the failover recording server's Recording Server service to start and the time it takes to connect to the cameras. In contrast, a hot standby recording server takes over faster because the Recording Server service is already running with the correct configuration and only has to start its cameras to deliver feeds. During the start up period, you can neither store recordings nor view live video from affected cameras.
- When a recording server becomes available again, it automatically takes over from the failover or hot standby recording server. Recordings stored by the failover or hot standby recording server are automatically merged into the standard recording server's databases. How long the merging process takes depends on the amount of recordings, on network capacity and more. During the merging process, you cannot browse recordings from the period during which the failover or hot standby recording server took over.
- If a failover recording server must take over from another recording server during the merging process in a regular failover recording server setup, it postpones the merging process with recording server A, and takes over from recording server B. When recording server B becomes available again, the regular failover recording server takes up the merging process with recording server A, after which it begins merging with recording server B.
In a hot standby setup, a hot standby server cannot take over for another recording server because it can only be hot standby for a single recording server. But if that recording server fails again, the hot standby takes over again and keeps the recordings from the previous period. The recording server keeps recordings until they are merged back to the primary recorder or until the failover recording server runs out of disk space.
- A failover solution does not provide complete redundancy. It can only serve as a reliable way of minimizing the downtime. If a recording server becomes available again, the Failover Server service makes sure that the recording server is ready to store recordings again. Only then is the responsibility for storing recordings handed back to the standard recording server. So, a loss of recordings at this stage of the process is very unlikely.
- Client users hardly notice that a failover recording server is taking over. A short break occurs, usually only for a few seconds, when the failover recording server takes over. During this break, users cannot access video from the affected recording server. Client users can resume viewing live video as soon as the failover recording server has taken over. Because recent recordings are stored on the failover recording server, they can play back recordings from after the failover recording server took over. Clients cannot play back older recordings stored only on the affected recording server until that recording server is functioning again and has taken over from the failover recording server. You cannot access archived recordings. When the recording server is functioning again, a merging process takes place during which failover recordings are merged back into the recording server's database. During this process, you cannot play back recordings from the period during which the failover recording server took over.
- In a regular failover setup, setting up one failover recording server as backup for another failover recording server is not necessary. This is because you do not allocate particular failover recording servers to take over from a standard recording server. Instead, you allocate failover groups. A failover group must contain at least one failover recording server, but you can add as many failover recording servers as needed. Provided a failover group contains more than one failover recording server, more than one failover recording server can take over. In a hot standby setup, you cannot set up a failover recording servers or hot standby servers for a hot standby server.

Install a failover recording server

Important: During the installation process, you are asked to specify a user account under which the *Failover Server* service should run. This user account must have administrator rights in the system. Note also that if you run workgroups, you should ignore the normal installation guidelines for installing recording servers and use the alternative installation method for workgroups.

Once you have installed the management server using the common installer, download the separate recording server installer from the management server's web page. As part of this installer, specify if you want to install a standard recording server or a failover recording server.

1. Go to the Management server's download web page and select the Recording Server installer. Save the installer somewhere appropriate and run it from here or run it directly from the web page.
2. Select the **Language** you want to use during the installation. Click **Continue**.
3. From the selection list, select **Failover** to install a recording server as a failover recording server.
4. Specify failover recording server properties. Click **Continue**.
5. When installing a failover recording server you must use the particular user account labeled *This account*. If needed, enter a password and confirm this. Click **Continue**.
6. Select **Files location** for the program file. In **Product language**, select the language in which to install your system. Click **Install**.
7. The software now installs. When done, you see a list of successfully installed components. Click **Close**.

When you have installed the failover recording server, you can check its state from the **Failover Server service** icon.

Setup and enable failover recording servers

Important: If you have disabled the failover recording server, you must enable it before it can take over from the standard recording servers.

Do the following to enable a failover recording server and edit its basic properties:

1. In the **Site Navigation** pane, select **Servers > Failover Servers**. This opens a list of installed failover recording servers and failover groups.
2. In the **Overview** pane, select the required failover recording server.
3. Right-click and select **Enabled**. The failover recording server is now enabled.
4. To edit failover recording server properties, go to the **Info** tab.
5. When done, go to the **Network** tab. Here you can define the failover recording server's public IP address and more. This is relevant if you use NAT (Network Address Translation) and port forwarding. See the standard recording server's **Network** tab for more information.

To see the status of a failover recording server, hold your mouse of the icon in the system tray. A tooltip appears containing the text entered in the Description field of the failover recording server. This may help you determine which recording server the failover recording server is configured to take over from.

Important: The failover recording server pings the management server on a regular basis to verify that it is online and able to request and receive the configuration of the standard recording servers when needed. If you block the pinging, the failover recording server is not able to take over from the standard recording servers.

Assign failover recording servers

On the **Failover** tab of a recording server, you can choose between 3 different types of failover setups:

- a** No failover setup
- b** A primary/secondary failover setup
- c** A hot standby setup.

If you select **b** and **c**, you must select the specific server/groups. With **b**, you can also select a secondary failover group. If the recording server becomes unavailable, a failover recording server from the primary failover group takes over. If you have also selected a secondary failover group, a failover recording server from the secondary group takes over in case all failover recording servers in the primary failover group are busy. This way you only risk not having a failover solution in the rare case when all failover recording servers in the primary, as well as in the secondary, failover group are busy.




1. In the **Site Navigation** pane, select *Servers >Recording Servers*. This opens a list of recording servers.
2. In the **Overview** pane, select the wanted recording server, go to the **Failover** tab.
3. To choose failover setup type, select either **None**, **Primary failover server group/Secondary failover sever group** or **Hot standby server**. You cannot select the same failover group as both primary and secondary failover group nor select regular failover servers already part of a failover group as hot standby servers.
4. Next, click **Advanced failover settings**. This opens the **Advanced Failover Settings** window, listing all devices attached to the selected recording server. If you selected **None**, Advanced failover settings are available. Any selections are kept for later failover setups.
5. To specify the level of failover support, select **Full Support**, **Live Only** or **Disabled** for each device in the list. Click **OK**.
6. In the **Failover service communication port (TCP)** field, edit the port number if needed.

Group failover recording servers

1. Select *Servers > Failover Servers*. This opens a list of installed failover recording servers and failover groups.
2. In the **Overview** pane, right-click the top-node *Failover Groups* and select *Add Group*.
3. Specify a name (in this example *Failover Group 1*) for and a description (optional) of your new group. Click **OK**.
4. Right-click the group (*Failover Group 1*) you just created. Select *Edit Group Members*. This opens the *Select Group Members* window.
5. Drag and drop or use the buttons to move the selected failover recording server(s) from the left side to the right side. Click **OK**. The selected failover recording server(s) now belongs to the group (*Failover Group 1*) you just created.
6. Go to the **Sequence** tab. Click **Up** and **Down** to set the internal sequence of the regular failover recordings servers in the group.

Read failover recording server status icons

The following icons represent the status of failover recording servers (icons are visible in the **Overview** pane):

Icon	Description
	The failover recording server is either waiting or "watching". When waiting, the failover recording server is not configured to take over from any recording server yet. When "watching", the failover recording server is configured to watch one or more recording servers.
	The failover recording server has taken over from the designated recording server. If you place your cursor over the server icon, you see a tooltip. Use the tooltip to see which recording server the failover recording server has taken over from.
	Connection to the failover recording server is broken.

Failover recording server properties

Specify the following failover recording server properties:

Name	Description
Name	The name of the failover recording server as it appears in the Management Client, logs and more.
Description	An optional field that you can use to describe the failover recording server, for example which recording server it takes over from.
Host name	Displays the network address of the failover recording server. You cannot change this.
UDP port	The port number used for communication between failover recording servers. By default, the system uses port 8844.
Database location	Specify the path to the database used by the failover recording server for storing recordings. You cannot change the database path while the failover recording server is taking over from a recording server. The system applies the changes when the failover recording server is no longer taking over from a recording server.
Enable this failover server	Clear to disable the failover recording server (selected by default). Note that you must disable failover recording servers before they can take over from recording servers.

Failover group properties

The **Info** tab:

Name	The name of the failover group is it appears in the Management Client, logs and more.
Description	An optional description, for example the server's physical location.

The Sequence tab:

Specify the failover sequence	Use Up and Down to set the wanted sequence of regular failover recording servers within the group.
--------------------------------------	--

About failover recording server services

A failover recording server has two services installed:

- A Failover Server service, which handles the processes of taking over from the recording server. This service is always running, and constantly checks the state of relevant recording servers.
- A Failover Recording Server service, which enables the failover recording server to act as a recording server.

In a failover group setup, this service is only started when required, that is when the regular failover recording server should take over from the recording server. Starting this service typically takes a couple of seconds, but may take longer depending on local security settings and more.

In a hot standby setup, this service is always running, allowing the hot standby server to take over faster than the regular failover recording server.

View status messages

1. On the failover recording server, right-click the *Failover Server service* icon.
2. Select *Show Status Messages*. The *Failover Server Status Messages* window appears, listing time-stamped status messages.

Change the management server address

The failover recording server must be able to communicate with your system's management server. You specify the IP address/hostname of the management server during the installation of the failover recording server. If you want to change the address of the management server, do as follows:

1. On the failover recording server, stop the Failover Recording Server service.
2. Right-click the notification area's Failover Recording Server service icon again.
3. Select *Change Settings*. The *Failover Recording Server Settings* window appears, so you can specify the IP address or host name of the management server with which the failover recording server should communicate.

View version information

Knowing the exact version of your *Failover Recording Server service* is an advantage if you need to contact product support.

1. On the failover recording server, right-click the *OnSSI Failover Recording Server service* icon.
2. Select *About*.
3. A small dialog box opens that shows the exact version of your *Failover Recording Server service*.

Failover management servers

About multiple management servers (clustering)

The management server can be installed on multiple servers within a cluster of servers. This ensures that the system has very little down-time. If a server in the cluster fails, another server in the cluster automatically takes over the failed server's job running the management server. The automatic process of switching over the server service to run on another server in the cluster only takes a very short time (up to 30 seconds).

It is only possible to have one active management server per surveillance setup, but other management servers may be set up to take over in case of failure.

The allowed number of failovers is limited to two within a six hour period. If exceeded, Management Server services are not automatically started by the clustering service. The number of allowed failovers can be changed to better fit your needs. See Microsoft®'s homepage for more information.

Prerequisites for clustering

- Two or more servers installed in a cluster:
 - Regarding clusters in Microsoft Windows 2008®, see Failover clusters.
- **Either** an external SQL database installed **outside** the server cluster **or** an **internal** SQL (clustered) service within the server cluster (creating an internal SQL service requires the use of SQL Server Standard or a greater version which is capable of working as a clustered SQL Server).
- A Microsoft® Windows® Server (Enterprise or Data Center edition).

Install in a cluster

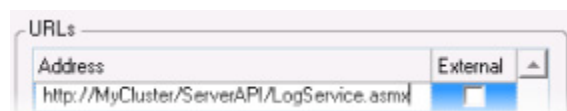
Descriptions and illustrations might differ from what you see on your screen.

Installation and change of URL address:

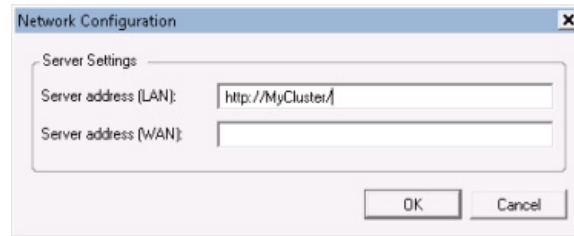
1. Install the management server and all its subcomponents on the first server in the cluster.

The management server must be installed with a specific user and not as a network service. This requires that you use the Custom install option. Also, the specific user must have access to the shared network drive and preferably a non-expiry password.

2. After you have installed the management server and the Management Client on the first server in the cluster, open the Management Client, and from the *Tools* menu, select *Registered Services*.
 - a) In the *Add/Remove Registered Services* window, select *Log Service* in the list, click *Edit*.
 - b) In the *Edit Registered Service* window, change the URL address of the log service to the URL address of the cluster.



- c) Repeat steps a and b for all services listed in the *Add/Remove Registered Services* window. Click *Network*.
- d) In the *Network Configuration* window, change the URL address of the server to the URL address of the cluster. (This step only applies to the first server in the cluster.) Click *OK*.



3. In the *Add/Remove Registered Services* window, click *Close*. Exit the Management Client.
4. Stop the management server service and the IIS. Read about how to stop the IIS at Microsoft's® homepage.
5. Repeat steps 1-4 for all subsequent servers in the cluster, this time pointing to the existing SQL database. However, for the **last** server in the cluster on which you install the management server, do not stop the Management Server service.

Next, in order to take effect, the Management Server service must be configured as a generic service in the failover cluster:

1. On the last server on which you have installed the management server, go to *Start, Administrative Tools*, open Windows' *Failover Cluster Management*. In the *Failover Cluster Management* window, expand your cluster, right-click *Services and Applications*, and select *Configure a Service or Application...*.



2. In the *High Availability* dialog box click *Next*, select *Generic Service* and click *Next*. Do not specify anything on the third page of the dialog box, click *Next*.
3. Select the *RC-L_RC-E Management Server service*, click *Next*. Specify the name (host name of the cluster) that clients use when accessing the service, click *Next*.
4. No storage is required for the service, click *Next*. No registry settings should be replicated, click *Next*. Verify that the cluster service is configured according to your needs, click *Next*. The management server is now configured as a generic service in the failover cluster. Click *Finish*.
5. In the cluster setup, the Data Collector should be set as a dependent service of the management server, so the service stops when the management server is stopped.
6. To add the *RC-L_RC-E Data Collector Server service* as a resource to the *RC-L_RC-E Management Server Cluster* service, right-click the cluster service and click *Add a resource > 4 - Generic Service* and *RC-L_RC-E_Data Collector Server*.

The service channel and the IIS should both be installed normally with the exact same user, and not as cluster services.

Upgrade in a cluster

Make sure to have a backup of the database before updating the cluster.

1. Stop the Management Server services on all management servers in the cluster.
2. Uninstall the management server on all servers in the cluster.

3. Use the procedure for installing multiple management servers in a cluster as described for install in a cluster, see Install in a cluster (on page 138).

Important: When installing, make sure to reuse the existing SQL configuration database (which is automatically upgraded from the old existing database version to the new one).

Remote connect services

About remote connect services

Available functionality depends on the recorder you are using. See Differentiate LS and ES Recorders (on page 13) for more information.

The remote connect services feature contains the Axis One-click Camera Connection technology developed by Axis Communications. It enables the system to retrieve video (and audio) from external cameras where firewalls and/or router network configuration normally prevents initiating connections to such cameras. The actual communication takes place via secure tunnel servers (ST servers). ST servers use VPN. Only devices that hold a valid key work within a VPN. This offers a secure tunnel where public networks can exchange data in a safe way.

Remote connect services allows you to:

- Edit credentials within the Axis Dispatch Service
- Add, edit, and remove ST servers
- Register/unregister and edit Axis One-click cameras
- Go to the hardware related to the Axis One-Click camera.

Before you can use Axis One-click Camera Connection, you must first install a suitable ST server environment. To work with secure tunnel server (ST server) environments and Axis One-click cameras, you must first contact your system provider to obtain the needed user name and password for Axis Dispatch Services.

Install STS environment for One-click camera connection

Prerequisites:

- Contact your system provider to obtain the needed user name and password for Axis Dispatch Services
 - Make sure your camera(s) support Axis Video Hosting System. Go to <http://www.axis.com/products/avhs/>.
 - If needed, update your Axis cameras with the newest firmware. Go to <http://www.axis.com/techsup/firmware.php>
1. On each camera's homepage, go to *Basic Setup*, *TCP/IP*, and select *Enable AVHS* and *Always*
 2. From your management server's download web page, install the *Axis One-Click Connection Component* to setup a suitable Axis secure tunnel framework.

Add/edit STSs

1. Do one of the following:
 - a) To add an ST servers, right-click the *Axis Secure Tunnel Servers* top node, select *Add Axis Secure Tunnel Server*.
 - b) To edit an ST server, right-click it, select *Edit Axis Secure Tunnel Server*.
2. In the window that opens, fill in the relevant information.
3. If you chose to use credentials when you installed the *Axis One-Click Connection Component*, select the *Use credentials* check box and fill in the same user name and password as used for the *Axis One-Click Connection Component*.

4. Click OK.

Register new Axis One-click camera

1. To register a camera under an ST server, right-click it and select *Register Axis One-click Camera*.
2. In the window that opens, fill in the relevant information and click *OK*. The camera now appears under the relevant ST server.

The camera can have the following color codings:

Color	Description
Red	Initial state. Registered, but not connected to the ST server.
Yellow	Registered. Connected to the ST server, but not added as hardware.
Green	Added as hardware. May or may not be connected to the ST server.

When you add a new camera, its status is always green. The connection status is reflected by *Devices on Recording Servers* in the **Overview** pane. In the **Overview** pane, you may group your cameras for an easier overview. If you choose **not** to register your camera at the Axis dispatch service at this point, you can do so later from the right-click menu (select *Edit Axis One-click Camera*).

Axis One-Click Camera connection properties

Name	Description
Camera password	Enter/edit. Provided with your camera at purchase. For further details, see your camera's manual or www.axis.com .
Camera user	See details for <i>Camera password</i> .
Description	Enter/edit a description for the camera.
External address	Enter/edit the http address of the ST server to which the camera(s) connect.
Internal address	Enter/edit the http address of the ST server to which the recording server connects.
Name	If needed, edit the name of the item.
Owner authentication key	See <i>Camera password</i> .
Passwords (for Dispatch Server)	Enter password. Must be identical to the one received from your system provider.
Passwords (for ST server)	Enter password. Must be identical to the one entered when the <i>Axis One-Click Connection Component</i> was installed.
Register/Unregister at the Axis Dispatch Service	Indicate whether you wish to register your Axis camera with the Axis dispatch service. Can be done at time of setup or later.
Serial number	Hardware serial number as specified by the manufacturer. The serial number is often, but not always, identical to the MAC address.
Use credentials	Select the check box if you decided to use credentials during the installation of the ST server.
User name (for Dispatch Server)	Enter a user name identical to the one received from your system provider.
User name (for ST server)	Enter user name. Must be identical to the one entered when the <i>Axis One-Click Connection Component</i> was installed

OnSSI Federated Architecture

About selecting Interconnect or OnSSI Federated Architecture

Ocularis was designed where users on the central site need to access the video directly on the remote site. The Ocularis ES RC-E recording component can extend this distributed environment to the Management Server. Options include: Interconnect or OnSSI Federated Architecture.

Use OnSSI Federated Architecture when:

- The network connection between the central and remote sites is a stable.
- The network uses the same domain.
- There are fewer larger sites.

Use Interconnect when:

- The network connection between the central and remote sites is unstable.
- You or your organization want to use another product on the remote sites.
- The network uses different domains or workgroups.
- There are many smaller sites.

About OnSSI Federated Architecture

Ocularis LS cannot run as a central site.

OnSSI Federated Architecture links multiple individual standard systems into a parent/child hierarchy of sites. With this configuration, client users with sufficient rights have seamless access to video, audio and other resources across individual sites. Through a single login, administrators can centrally manage all sites within the federated hierarchy, based on administrator rights for the individual sites.

Important: You can only centrally manage a federated hierarchy if all sites use the same version of recording component.

You install and configure each site in a federated hierarchy as a normal standalone system with standard system components, settings, rules, schedules, administrators, users, and user rights. Once you have installed each site, you connect these by requesting a federated link from one site (the parent site) to another (the child site). When the link is established, the two sites automatically create a federated hierarchy to which you can add more sites to grow the federated hierarchy. Once you have created a federated hierarchy, it allows users and administrators logged into a site to access that site and any child or sub-child sites it may have. Access to child sites depend on the user rights.

Important: You can only add sites that use the same version recording component as the site you are adding to.

You can only have one parent site, but the parent site can have an unlimited number of child sites. The link between a parent site and a child site is established, when you request the link from the parent site. If you are not the administrator of the child site, the request must be accepted by the child site administrator. A parent site includes information about all of its child sites and the child sites' child sites, but only controls them one level down. Similarly, a child site only knows about and answers to its parent site one level up. Your home site is the parent site you are logged in to.




A parent site contains an updated list of all its currently attached child sites, child sites' child sites and so on. The federated hierarchy has a regularly scheduled synchronization between sites, as well as management-triggered synchronization every time a site is added or removed. When the system synchronizes the hierarchy, it takes place level by level, each level forwarding and returning communication, until it reaches the server that requests the information. The system sends less than 1MB each time. Depending on the number of levels, changes to a hierarchy can take some time to become visible in the Management Client. You cannot schedule your own synchronizations.

Data traffic

The system sends video or configuration data when a user or administrator views live or recorded video or configures a site. The amount of data depends on what and how much is being viewed.

Status icons in OnSSI Federated Architecture

When you work with federated architecture, you may see the following number of icons that represent the different states in which a site can be:

Description	
	The top site in the entire hierarchy is operational.
	The top site in the entire hierarchy is still operational, but one or more issues need attention. Shown on top of the top site icon.
	The home site is operational.
	The site is awaiting to be accepted in the hierarchy.
	The site is attaching, but is not yet operational.

Set up your system to run federated sites

To prepare your system for federated architecture you must make certain choices when you install the management server. Depending on how your system is set up, choose between three different alternatives.

Alternative 1: Connect sites from the same domain (with a common domain user) and customize the installation of the management server to federated architecture

Before you install the management server, you should create a common domain user and use this as the administrator on all computers involved in the federated architecture.

Custom installation

1. Start the management server installation and select **Custom**.
2. Select to install the Management Server service using a user account. The selected user account must be the administrator on all management servers and you must also use this when you install the other management servers in the federated architecture setup.
3. Finish the installation. Repeat steps 1-3 to install any other systems you want to connect in the federated architecture.

Single Server or Distributed Installation - set up network service on all servers

1. Start the management server installation and select **Single Server** or **Distributed**. This installs the management server as a *network service*. Repeat step 1 to install any other systems you want to connect with the federated architecture.
2. Connect to the management server you want to have as your parent site in the Management Client.
3. Expand *Security > Roles > Administrator*.
4. Add the child computer to this parent server's *Administrator* role.
5. Log out of the parent management server and connect to the management server that you just added as a child.
6. In the Overview pane, click *Administrator*.
7. Add the parent computer to this servers *Administrator* role.
8. Log out of the management server and connect to the parent management server.

Alternative 2: Connecting sites from different domains

To connect to sites across domains, make sure that these domains are trusted by each other. Setting up domains to trust each other has nothing to do with federated, but has to do with Microsoft Windows Domain configuration. When

you have established trust between the domains on which the sites you want to connect to each other in a federated hierarchy, follow the same description as seen in Alternative 1. For more information about how to set up trusted domains, see the Microsoft website.

Use Interconnect for creating multi-site systems when your system works with multiple domains.

Alternative 3: Connect sites in workgroup(s)

When you connect sites inside workgroups, federated architecture must have the same administrator account present on all computers you want connected in the federated architecture to work properly. You must have this in place before installing the system.

1. Log in to *Windows* using a common administrator account.
2. Start the management server installation and click *Custom*.
3. Select to install the Management Server service using a common administrator account.
4. Finish the installation. Repeat steps 1-4 to install any other systems you want to connect. You must all of these systems using a common administrator account.


Use Interconnect for creating multi-site systems when the sites are not part of a domain.


You cannot mix domain(s) and workgroup(s). This means that you cannot connect sites from a domain to sites from a workgroup and vice versa.

Add site to hierarchy

You can add child sites to both your home site and to its child sites, if you are connected to any of these.

1. Select the Federated Site Hierarchy pane.
2. Select the site to which you want to add a child site, right-click, and click *Add Site to Hierarchy*.
3. Enter the URL of the requested child in the *Add Site to Hierarchy* window and click *OK*.
4. The parent site sends a link request to the child site and after a while, a link to the new child site is added to the Federated Sites Hierarchy pane.
5. If you can establish the link to new child site without requesting acceptance from the child site administrator, go to step 7.


If **not**, the new child site has the awaiting acceptance  icon and the child site administrator must authorize the request.

6. Make sure the child site's administrator authorizes the link request from the child site. See *Accept inclusion in hierarchy* (on page 144).
7. The new parent/child link is established and the Federated Sites Hierarchy pane is updated with the  icon for the new child.

Accept inclusion in hierarchy

When a child site has received a link request from the potential parent site, it has the awaiting acceptance  icon.

To accept a child link request:

1. In the Management Client window, in the Federated Sites Hierarchy pane, select the requesting site, right-click, and click **Accept Inclusion in Hierarchy**.
2. Click *Yes*.
3. The new parent/child link is established and the Federated Sites Hierarchy pane is updated with the normal site  icon for the selected site.

Changes made to child sites located far from your home-site might take some time to be reflected in the Federated Sites Hierarchy pane.

Refresh site hierarchy

The system performs automatic synchronization of the hierarchy regularly through all levels of your parent/child setup. You can refresh if you want a current overview of the sites in the hierarchy, and do not want to wait for the next automatic synchronization.

When you refresh, the home-site displays a current overview of the sites in the hierarchy from the home site's point-of-view. Only changes saved by the home-site since the last synchronization are reflected.

1. To refresh, right-click the home site in the Federated Site Hierarchy pane and click **Refresh Site Hierarchy**.
2. Changes further down in the hierarchy are not reflected. To see them, await a full automatic synchronization.

Connect to another site in hierarchy

If you have administrator rights, you can connect to other sites and administrate these.

1. Click the relevant site in the Federated Site Hierarchy pane.

A brief dialog box informs you that you are being connected to the selected site.

2. When connection is complete, your view in the Federated Sites Hierarchy pane changes to reflect that you are connected to a different site.

In this example, the user logged into the home site *Rome Server* and connected to the child *Paris Server*:



Detach a site from the hierarchy

The process of detaching or removing a site from its hierarchy depends on the site you want to detach.

When you detach a site, the link between the sites are broken. If a site has child sites, it becomes the parent site.



The detach site option is only available if a site is the child site of another site.

Detach a child site from the hierarchy

You do not have to connect to a site to detach it.

1. In the **Federated Sites Hierarchy** pane, right-click the site you want to detach and select *Detach Site from Hierarchy*.
2. Click Yes to remove the detached site and update the *Federated Sites Hierarchy* pane.

Detach a home site from the hierarchy

1. In the **Federated Sites Hierarchy** pane, right-click the home site, and click *Detach Site from Hierarchy*.
2. Click Yes to update the *Federated Sites Hierarchy* pane. If the detached site has child sites, it becomes the new top site for this branch of the hierarchy, and the normal site icon  changes to a top site  icon.
3. Click OK.

Changes to the hierarchy are reflected after a manual refresh or an automatic synchronization.

Federated site properties

General tab

You can change information related to the site you are currently connected to.

Name	Description
Name	Enter the name of the site.
Description	Enter a site description.
URLs	Use the list to add and remove URL(s) for this site and indicate whether they are external and not.
Version	The version number of the site's management server.
Service account	The service account under which the management server is running.
Time for last synchronization	Time and date of the last synchronization of the hierarchy.
Status for last synchronization	The status of the last synchronization of the hierarchy. It can be either <i>Successful</i> or <i>Failed</i> .

Parent Site tab

This tab shows information about the parent site of the site you are currently connected to.

Name	Description
Name	Enter the name of the site.
Description	Shows a description of the parent.
URLs	Lists URL(s) for this parent and indicates whether they are external or not.
Version	The version number of the site's management server.
Service account	The service account under which the management server is running.
Time for last synchronization	Time and date of the last synchronization of the hierarchy.
Status for last synchronization	The status of the last synchronization of the hierarchy. It can be either <i>Successful</i> or <i>Failed</i> .

Interconnect

About selecting Interconnect or OnSSI Federated Architecture

Ocularis was designed where users on the central site need to access the video directly on the remote site. The Ocularis ES RC-E recording component can extend this distributed environment to the Management Server. Options include: Interconnect or OnSSI Federated Architecture.

Use OnSSI Federated Architecture when:

- The network connection between the central and remote sites is a stable.
- The network uses the same domain.
- There are fewer larger sites.

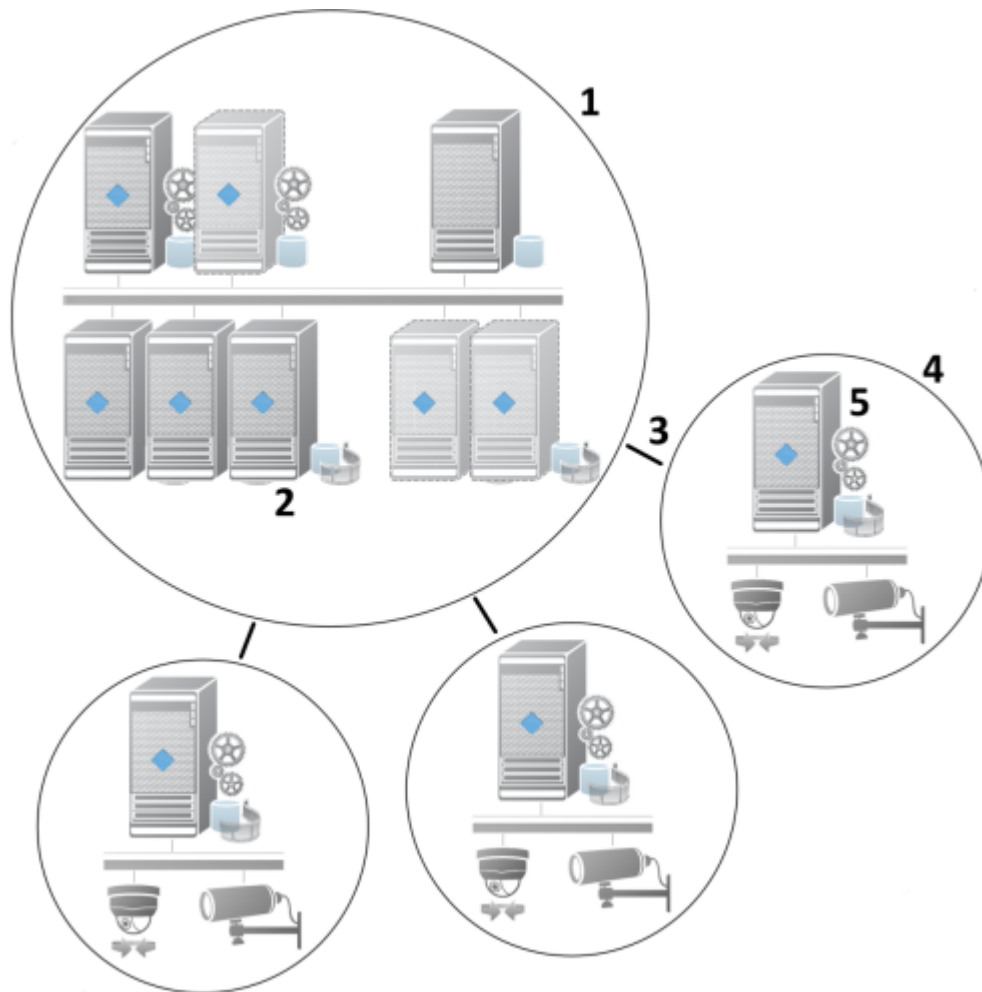
Use Interconnect when:

- The network connection between the central and remote sites is unstable.
- You or your organization want to use another product on the remote sites.
- The network uses different domains or workgroups.
- There are many smaller sites.

About Interconnect

Interconnect allows you to integrate a number of smaller, physically fragmented, and remote recorder installations with an Ocularis ES central site. You can install these smaller sites, called remote sites, on mobile units, for example, boats, busses or trains. This means that such sites do not need to be permanently connected to a network.

The following illustration shows how you could set up Interconnect on the system:



1. Interconnect central Ocularis ES site
2. Interconnect drivers (handles the connection between the central sites' recording servers and the remote site, must be selected in the list of drivers when adding remote systems via the **Add Hardware** wizard)
3. Interconnect connection
4. Interconnect remote site (the complete remote site with system installation, users, cameras and so on)
5. Interconnect remote system (the actual technical installation at the remote site)

Each remote site runs independently and can perform any normal surveillance tasks. Depending on the network connections and appropriate user rights, Interconnect™ offers you direct live viewing of remote site cameras and play back of remote site recordings from the central site. It also offers you the possibility to transfer remote site recordings to the central site based on either events, rules/schedules, or manual requests by Ocularis Client users. It also allows central site users to employ events originally triggered on remote sites on the central site.

Which recorder can act as central site and which can act as remote sites depends on the specific setup. It differs from setup to setup which versions, how many cameras, and how devices and events originating from the remote site are handled - if at all - by the central site.

You add remote sites to the central site by using the **Address range scanning** or **Manual** options in the **Add Hardware** (on page 45) wizard. When you add the remote site, you must specify an account on the remote site. This account can be either a basic user, local Windows user, or domain user. You can reuse an existing user or create a new one to use with Interconnect. You must create a new user on the remote system before creating the Interconnect setup. Depending on the user rights for the selected user on the remote site, the central site gets access to all cameras and functions or a sub-set of them.

About possible Interconnect setups

There are multiple ways to run Interconnect.

In the following, the three most likely scenarios are described. How to run your setup depends on your network connection, whether you request playback, and whether you retrieve remote recordings and to what degree.

Direct playback from remote sites on request (good network connections)

The most straight forward setup. The central site is continuously online with its remote sites which send remote recordings on request. Central site users play back remote recordings directly from the remote sites. This requires use of the **Play back recordings from remote system** option.

Rule-based retrieval of selected remote recording sequences from remote sites (periodically limited network connections)

Used when selected recording sequences (originating from remote sites) should be stored centrally to ensure independence from remote sites. Independence is crucial in case of network failure or network restrictions. Configuring retrieval of remote recordings when the network connection is optimal, that is not used for other priority data, can be done from the **Remote Recordings** tab.

After connection failure, missing remote recordings are per default retrieved from remote sites

Uses remote sites like a recording server uses the edge storage on a camera. Typically, remote sites are on-line with their central site, feeding it a live stream that the central site records. Should the network fail for some reason, the central site miss out on recording sequences. However, once the network is re-established, the central site automatically retrieves remote recordings covering the down-period. This requires use of the **Automatically retrieve remote recordings when connection is restored** option.

You can mix any of the above solutions to fit your organizations special needs.

Interconnect and licensing

Cameras under remote sites in an Interconnect setup are listed on the **License Information** page of the central site. They are listed according to the same rules as other cameras, but with Interconnect in front:

- **Interconnect Camera**

Update remote site hardware

1. On the central site, expand **Servers** and select **Recording Servers**.

2. In the Overview pane, expand the required recording server, select the relevant remote system. Right-click it.
3. Select **Update Hardware**. This opens the **Update hardware** dialog box.
4. The dialog box lists all changes (devices removed, updated and added) in the remote system since your Interconnect setup was established or refreshed last. Click **Confirm** to update your central site with these changes.

Establish remote desktop connection to remote system

Preconditions: The remote desktop connections to the computer you want to remote to must be up and running and its management application must be open.

1. On the central site, expand **Servers** and select **Recording Servers**.
2. In the Overview pane, expand the required recording server, select the relevant remote system.
3. In the Properties pane, select the **Info** tab.
4. In the **Remote administration** area, type the appropriate Windows user name and password.
5. Once user name and password are saved, click **Connect** to establish remote desktop connection.
6. In the toolbar, click **Save**.

Enable playback directly from remote site camera

1. On the central site, expand **Servers** and select **Recording Servers**.
2. In the Overview pane, expand the required recording server, select the relevant remote system. Select the relevant camera.
3. In the Properties pane, select the **Record** tab, and select the **Play back recordings from remote system** option.
4. In the toolbar, click **Save**.

In an Interconnect setup, the central system disregards privacy masking defined in a remote system.

Retrieve remote recordings from remote site camera

1. On the central site, expand **Servers** and select **Recording Servers**.
2. In the Overview pane, expand the required recording server, select the relevant remote system. Select the relevant camera.
3. In the Properties pane, select the **Record** tab, and select the **Automatically retrieve remote recordings when connection is restored** option.
4. In the toolbar, click **Save**.

In an Interconnect setup, the central system disregards privacy masking defined in a remote system.

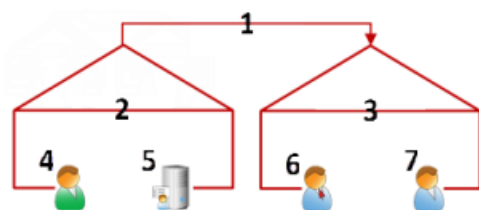
Multi-domain with one-way trust

Setup with one-way trust

If you run your system in a multi-domain environment, you can configure this setup with one-way trust. The system is installed on the **trusting** domain and users log in from **trusting** and **trusted** domains.

1. Create a service account in the **trusted** domain. You can name it whatever you want, for example, *svcOnSSI*.
2. Add the new service account to the following local Windows user groups on the server running the system, in the **trusting** domain:
 - o Administrators
 - o IIS_IUSRS (Windows Server 2008, necessary for Internet Information Services (IIS) Application Pools)
 - o IIS_WPG (Windows Server 2003, necessary for IIS Application Pools).
3. Make sure that the service account has system administrator rights on your SQL Database or SQL Server Express, either directly or through the **BUILTIN\Administrators** group.
4. Set the identity of the *ManagementServerAppPool* Application Pool in the IIS to the service account.
5. Reboot the server to make sure that all group membership and permission changes take effect.

Important: To add **trusted** domain users to new or existing system roles, log in to Windows as a **trusted** domain user. Next, launch the Management Client and log in as user of either the **trusting** domain or the **trusted** domain. If you log in to Windows as a **trusting** domain user, you are asked for credentials for the **trusted** domain in order to browse for users.



Example illustration of multi-domain environments with one-way trust.

Legend:

1. One-way outgoing domain trust
2. MyDomain.local
3. OtherDomain.edu
4. Trusting domain user
5. Management server
6. OnSSI service account
7. Trusted domain user

SNMP

About SNMP support

Available functionality depends on the recorder you are using. See Differentiate LS and ES Recorders (on page 13) for more information.

Your system supports Simple Network Management Protocol (SNMP), a standard protocol for monitoring and controlling network devices, for managing their configuration, collecting statistics and more.

The system acts as an SNMP agent, which can generate an SNMP trap as a result of a triggered rule. A third-party SNMP management console can then receive information about the rule-triggering event, and operators of the SNMP management console can configure their system for further action as required.

The implementation uses Microsoft® Windows® SNMP Service for triggering SNMP traps. This means that you must install the SNMP Service on recording servers.

Install SNMP service

1. On the relevant recording servers, open Windows' **Programs and Features** functionality.
2. In the left side of the **Programs and Features** dialog box, click *Turn Windows functionality on or off*. This opens the *Windows feature* window.
3. In the dialog box, select the check box next to *Simple Network Management Protocol (SNMP)* and click *OK*.

Configure SNMP service

1. On the required recording servers, select *Start > Control Panel > Administrative Tools > Services*.
2. Double-click the SNMP Service.
3. Select the *Traps* tab.
4. Specify a community name, and click *Add to list*.
5. Select the *Destinations* tab.
6. Click *Add*, and specify the IP address or host name of the server running your third-party SNMP management station software.
7. Click *OK*.

Ocularis CS servers

About Ocularis CS servers

This section is only relevant if you use:

- Ocularis ES
- you have installations with Ocularis CS version 7 or later.

You can add Ocularis CS servers to your Ocularis ES system. When added, the servers act as recording servers and their video can be viewed by the clients.

In the Management Client, you can see the status of added Ocularis CS servers. You must still define all Ocularis CS server settings (cameras, scheduling, user rights etc.) in Ocularis CS's Management Application. See the Ocularis CS documentation.

To give users access to video from Ocularis CS servers, you must match roles in Ocularis ES with user rights defined on the Ocularis CS servers.

- Add Ocularis CS servers (see "Add Ocularis CS servers" on page 152)
- Define roles with access to Ocularis CS servers (see "Define roles with access to Ocularis CS servers" on page 152)
- Edit Ocularis CS servers (see "Edit Ocularis CS servers" on page 152)

Add Ocularis CS servers

Even if the Ocularis CS system has an internal master/slave setup, you cannot reuse it in your Ocularis ES system. You must add each Ocularis CS server that you need device data from individually.

To add an existing Ocularis CS server to your system:

1. From the Management Client's **Tools** menu, select **OnSSI Compatible Recording Servers**.
2. In the **Add/Remove** dialog box, click **Add**.
3. Enter the IP address or the host name of the Ocularis CS server.
4. Enter the port number used by the Ocularis CS server.
The default port number is 80. If in doubt, you can find the port number in Ocularis CS's Management Application under Server Access.
5. Enter the user credentials for the administrator of the Ocularis CS server to give yourself unlimited rights to the device data from it.
6. If the Ocularis ES system accesses the Ocularis CS server through an Internet connection, click **Network** to specify the WAN address of Ocularis ES's management server. You need only define the WAN address once.

Next step is to give your users access to devices from the Ocularis CS server.

Define roles with access to Ocularis CS servers

To give the users access to devices from the added Ocularis CS servers:

1. On the Ocularis CS server, open the Management Application to find an Ocularis CS user who has user rights you can reuse and match with a role in your Ocularis ES system. If not, create a new Ocularis CS user that matches the role in your Ocularis ES system.
2. Take careful note of the Ocularis CS user's user name, password and authentication type (basic or Windows). The Ocularis ES system does not verify that the information you specify later in these steps corresponds to a defined user in Ocularis CS.
3. In the Ocularis ES Management Client's **Site Navigation** pane, expand **Security**, and select **Roles**.
4. Select the role you want to use or define a new role.
5. At the bottom of the **Role Settings** pane, select the **Servers** tab and then the Ocularis CS server under OnSSI Compatible Recording Servers.
6. Select the Ocularis CS user with the user rights you want to match with your role.
7. Click **Save**.

Edit Ocularis CS servers

To edit an Ocularis CS server added to your system:

1. From the **Tools** menu, select **OnSSI Compatible Recording Servers**.
2. Select the Ocularis CS server from the list, and click **Edit**.
3. Edit the relevant settings and click **OK**.

System maintenance

Ports used by the system

If nothing else is mentioned, the ports are both inbound and outbound. The port numbers are the default numbers. You can change the port numbers if needed.

Port number	Protocol	Used by	Purpose
20 and 21	FTP	Recording servers	Listening for event messages from devices.
25	SMTP	Recording servers	Listening for event messages from devices and for sending images to the surveillance system server via e-mail.
80	HTTP	The IIS on the management server	Running the Management Server service.
443	HTTPS	Management server and service channel	Authentication of basic users.
554	RTSP	Recording servers	Traffic that controls streaming from cameras.
1024 and higher (except the ports mentioned below)	HTTP	Recording servers	Outbound only. Traffic between cameras and servers.
1433	TCP	All processes in the system (among others management server and log server)	Communication with the SQL Server.
5210	TCP	Recording servers and failover recording servers	Merging of databases after a failover recording server has been running.
5432	TCP	Recording servers	Listening for event messages from devices.
7563	TCP	Recording servers and Ocularis Client	Communication with the Image Server interface. Also handling of PTZ camera control commands and for retrieving image streams from clients etc.
7609	HTTP	Report server and Data Collector Server service	Communication between the two. The port must always be kept open on the server running the Data Collector Server service.

Port number	Protocol	Used by	Purpose
8080	UDP	Management server	Communication between internal processes on the server.
8844	UDP	Failover recording servers	Communication between the servers.
8990	TCP	Management server	Monitoring the status of the failover server service.
9993	TCP	Recording servers and management server	Communication between the two.
11000	TCP	Failover recording servers	Polling the state of recording servers.
12345	TCP	Management server and Ocularis Client	Communication between the system and NetMatrix recipients. You can change the port number in Management Client.
65101	UDP	Recording servers	Listening for event notifications from the drivers.

Backing up and restoring configuration

About backing up and restoring your system configuration

OnSSI recommends that you make regular backups of your system configuration as a disaster recovery measure. While it is rare to lose your configuration, it can happen under unfortunate circumstances. Luckily, it takes only a minute to back up your existing configuration.

The system offers a built-in feature that backs up all the system configuration you can define in the Management Client. Note that the log server database and the log files, including audit log files, are not included in this backup.

If your system is large, OnSSI recommends that you define scheduled backups. This is done with the third-party tool: Microsoft® SQL Server Management Studio. This backup includes the same data as a manual backup.

During a backup, your system stays online. Depending on your system configuration, your hardware, and on whether you have installed the SQL server and Management Client on a single server or several servers (a distributed setup), backing up the system configuration can take some time.

Each time you make a backup both manual and scheduled, the SQL Server's transaction log file is flushed. For additional information about how to flush this log file, go to <http://www.support.microsoft.com> and search for "SQL Server transaction log".

Back up log server database

Handle the *SurveillanceLogServer* database by using the method that you use when handling system configuration as described earlier. The *SurveillanceLogServer* database (the name may be different if you renamed the system configuration database) contains all your system logs, including errors reported by recording servers and cameras.

The database is located where the Log Server's SQL server is installed, typically the same place as your management server's SQL server. Backing up this database is not vital since it does not contain any system configuration, but you may later appreciate having access to system logs from before the management server backup/restore.

Manual backup and restore

About manually backing up your system configuration

When you want to perform a manual backup of your system configuration, make sure that your system stays online. Here are a few things to consider before you start the backup:

- You cannot use a backup to copy configurations to other systems.
- It can take some time to back up your configuration. It depends on your system configuration, your hardware, and on whether your SQL server, management server and Management Client are installed on the same computer.
- Logs, including audit logs, are **not** part of the configuration backup.

About back up/restore fail and problem scenarios

If, after your last system configuration backup, you have moved the other registered services such as the log server, you must select which registered service configuration you want for the new system. You can decide to keep the new configuration after the system is restored to the old version. You decide by looking at the host names of the services.

Back up system configuration manually

1. From the menu bar, select *File, Backup Configuration*.
2. Read the note in the dialog box and click *Backup*.
3. Enter a file name for the .cnf file.
4. Enter a folder destination and click *Save*.
5. Wait until the backup is finished and click *Close*.

Note: All relevant system configuration files are combined into one single .cnf file that is saved at a specified location. During the backup, all backup files are first exported to a temporary system backup folder on the management server. You can select another temporary folder by right-clicking the notification area's management server service icon and by selecting *Select shared backup folder*.

Restore system configuration from manual back up

Important information:

- Both the user who installs and the user who restores must be local administrator of the database on the management server **and** on the SQL server.
- Except for your recording servers, your system is completely shut down for the duration of the restore, which can take some time.

- A backup can only be restored on the system installation where it was created. Make sure that the setup is as similar as possible to when the backup was made. Otherwise, the restore might fail.
- If restoring fails during the validation phase, you can start the old configuration again because you have made no changes.
If restoring fails elsewhere in the process, you cannot roll back to the old configuration.
As long as the backup file is not corrupted, you can do another restore.
- Restoring replaces the current configuration. This means that any changes to the configuration since last backup are lost.
- No logs, including audit logs, are restored.
- Once restoring has started, you cannot cancel it.

Restoring:

1. Right-click the notification area's Management Server service icon and select *Restore Configuration*.
2. Read the important note and click *Restore*.
3. In the file open dialog box, browse to the location of the configuration backup file, select it, and click *Open*.

The backup file is located on the Management Client machine. If the Management Client is installed on a different server, copy the backup file to this server before you select the destination.

4. The *Restore Configuration* window opens. Wait for the restore to finish and click *Close*.

Select shared backup folder

Before backing up and restoring any system configuration, you must set a backup folder for this purpose.

1. Right-click the notification area's management server service icon and select *Select shared backup folder*.
2. In the window that appears, browse to the wanted file location.
3. Click OK twice.
4. If asked if you want to delete files in the current backup folder, click *Yes* or *No* depending on your needs

Scheduled backup and restore**About scheduled backup and restore of system configuration**

OnSSI recommends that you make regular backups of your system configuration as a disaster recovery measure. While it is rare to lose your configuration, it can happen under unfortunate circumstances. Luckily, it takes only a minute to back up your existing configuration. Regular backups also have the added benefit that they flush your Microsoft® SQL Server's transaction log.

If you have a smaller setup and do not need scheduled backups, you can back up your system configuration manually. For instructions, see Manual backup and restore of system configuration (see "Manual backup and restore" on page 155).

The management server stores your system's configuration in a database. When you back up/restore management server(s), make sure that this database is included in the backup/restore.

Prerequisites for using scheduled backup and restore

Microsoft® SQL Server Management Studio, a tool download-able for free from www.microsoft.com/downloads.

Apart from managing SQL Server databases, the tool includes some easy-to-use backup and restoration features. Download and install the tool on your management server.

Flush SQL server transaction log

Each time a change in the system's data occurs, the SQL Server log this change in its transaction log, regardless whether it is a SQL Server on your network or a SQL Server Express edition.

The transaction log is essentially a security feature that makes it possible to roll back and undo changes to the SQL Server database. By default, the SQL Server stores its transaction log indefinitely, and over time the transaction log build up more and more entries. The SQL Server's transaction log is by default located on the system drive, and if the transaction log keeps growing, it may in the end prevent Windows from running properly.

To avoid such a scenario, flushing the SQL Server's transaction log from time to time is a good idea. However, flushing it does not in itself make the transaction log file smaller, but it prevents it from growing out of control. Your system does not, however, automatically flush the SQL Server's transaction log at specific intervals. You can also do several things on the SQL Server itself to keep the size of the transaction log down.

For more information on this topic, go to support.microsoft.com (<http://www.support.microsoft.com>) and search for SQL Server transaction log.

Back up system configuration with scheduled backup

1. From Windows' *Start* menu, open Microsoft® SQL Server Management Studio by selecting *All Programs > Microsoft SQL Server 2008 > SQL Server Management Studio*.
2. When connecting, specify the name of the required SQL Server. Use the account under which you created the database.
- a) Find the *Surveillance* database that contains your entire system configuration, including recording servers, cameras, inputs, outputs, users, rules, patrolling profiles, and more.

We assume that the database uses the default name.

- b) Make a backup of the *Surveillance* database and make sure to:
 - Verify that the selected database is *Surveillance*
 - Verify that the backup type is **full**
 - Set the schedule for the recurrent backup
 - Verify that the suggested path is satisfactory or select alternative path
 - Select to **verify backup when finished** and to **perform checksum before writing to media**.
3. Follow the instructions in the tool to the end.

Also consider backing up the *SurveillanceLog* database by using the same method.

Restore system configuration from scheduled backup

Prerequisite: To prevent configurational changes being made while you restore the system configuration database, stop the:

- Management Server service (see "About the Management Server service and Recording Server service" on page 162)
- World Wide Web Publishing Service, also known as the Internet Information Service (IIS). Learn how to stop the IIS at: [http://technet.microsoft.com/en-us/library/cc732317\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc732317(WS.10).aspx).

Open Microsoft® SQL Server Management Studio from Windows' *Start* menu by selecting *All Programs > Microsoft SQL Server 2008 > SQL Server Management Studio*.

In the tool do the following:

1. When connecting, specify the name of the required SQL Server. Use the account under which the database was created.
2. Find the *Surveillance* database that contains your entire system configuration, including , recording servers, cameras, inputs, outputs, users, rules, patrolling profiles, etc.

3. Make a restore of the *Surveillance* database and make sure to:
 - Select to backup **from** device
 - Select backup media type **file**
 - Find and select your backup file *Surveillance.bak*
 - Select to **overwrite the existing database**.
4. Follow the instructions in the tool to the end.

If you also backed up the *SurveillanceLog* database from the old log server, restore it on the new log server by using the same method.

Note that the system does not work while the Management Server service is stopped. It is important to remember to start the services again once you have finished restoring the database.

Moving the management server

About moving the management server

You may sometimes need to move the management server installation from one physical server to another. The management server stores your system configuration in a database. If you are moving the management server from one physical server to another, it is vital that you make sure that your new management server also gets access to this database. The system configuration database can be stored in two different ways:

- **Network SQL Server:** If you are storing your system configuration in a database on an existing SQL Server on your network, you can point to the database's location on that SQL Server when installing the management server software on your new management server. In that case, only the following paragraph about management server hostname and IP address applies and you should ignore the rest of this topic:
Management server hostname and IP address: When you move the management server from one physical server to another physical server, it is by far the easiest to give the new server the same hostname and IP address as the old one. This is due to the fact that the recording server connects to the hostname and IP address of the old management server. If you have given the new management server a new hostname and/or IP address, the recording server cannot find the management server. Manually stop each recording server in your system, change their management server URL, and when done, restart them.
- **Local SQL Server:** If you are storing your system configuration in a local SQL Server database on the management server itself, it is important that you back up the existing management server's system configuration database before the move. By backing up the database, and subsequently restoring it on the new server, you avoid having to reconfigure your cameras, rules, time profiles, etc. after the move.

Prerequisites

- **Your software installation file for installation on the new management server.**
- **Your initial license (.lic) file**, that is the one you used when initially installing your system, not the .lic file which is the result of your license activation (see "Activate licenses offline" on page 31). License activation is, among other things, based on the specific hardware on which the activation took place. Therefore an activated .lic file cannot be reused when moving to a new server. Note that if you are also upgrading your system software in connection with the move, you received a new initial .lic file together with your new Software License Code (SLC).
- **Local SQL Server users only: Microsoft® SQL Server Management Studio.**
- What happens while the management server is unavailable? (see "About unavailable management servers" on page 159)
- Copy log server database (see "Back up log server database" on page 155)

About unavailable management servers

- **Recording servers can still record:** Any currently working recording servers received a copy of their configuration from the management server, so they can work and store recordings on their own while the management server is down. Scheduled and motion-triggered recording therefore works, and event-triggered recording works unless based on events related to the management server or any other recording server because these go through the management server.
- **Recording servers temporarily store log data locally:** They automatically send log data to the management server when it becomes available again.
 - **Clients cannot log in:** Client access is authorized through the management server. Without the management server, clients cannot log in.
 - **Clients that are already logged in can remain logged in for up to one hour:** When clients log in, they are authorized by the management server and can communicate with recording servers for up to one hour. If you can get the new management server up and running within an hour, many of your users are not affected.
 - **No ability to configure the system:** Without the management server, you cannot change the system configuration.

OnSSI recommends that you inform your users about the risk of losing contact with the surveillance system while the management server is down.

Move the system configuration

Moving your system configuration is a three step process:

1. Make a backup of your system configuration. This is identical to making a scheduled backup (see "Back up system configuration with scheduled backup" on page 157).
2. Install the new management server on the new server. See scheduled backup, step 2.
3. Restore your system configuration to the new system. See Restore system configuration from scheduled backup (on page 157).

Managing the SQL server

About updating the SQL server address

When you install a system as a trial, or if you restructure a large installation, you may need to use a different SQL database. You can do this with the **Update SQL Server Address** tool.

With the tool, you can change the addresses of the SQL servers used by the management server and the log server. The only limitation is that you cannot change the management server SQL address at the same time as the log server's SQL address. You can do it one after another.

You must do SQL updates locally on the computer where you have installed the management server **or** log server. You cannot do it from the Management Client. I

You must copy the SQL databases before you proceed.

Update the log server's SQL address

Management server and log server located on the same computer

1. Go to the computer where your management server is installed.
2. Go to the notification area of the taskbar. Right-click the **Management Server** icon, select **Update SQL address**. The **Update SQL Server Address** dialog box appears.
3. Select **Log Server** and click **Next**.
4. Enter or select the new SQL server and click **Next**.

5. Select the new SQL database and click **Select**.
6. Wait while the address change takes place. Click **OK** to confirm.

Management server and log server located on different computers

1. Go to the computer where your management server is installed and copy the directory `%ProgramFiles%\OnSSI\RC-L_RC-E Management Server\Tools\ChangeSqlAddress\` (with content) to a temporary directory on another server.
2. Paste the directory that you copied to a temporary place on the computer where the log server is installed and run the included file: `VideoOS.Server.ChangeSqlAddress.exe`. The **Update SQL Server Address** dialog box appears.
3. Select **Log Server** and click **Next**.
4. Enter or select the new SQL server and click **Next**.
5. Select the new SQL database and click **Select**.
6. Wait while the address change takes place. Click **OK** to confirm.


Replace hardware

When you replace a hardware device on your network with another hardware device, you must know the IP address, port, user name and password of the new hardware device.

Your system might be affected by license limitations. Using the **Activate Online** wizard, you must reactivate your licenses **after** replacing hardware devices. If the new number of cameras exceeds the old number of cameras, you might also have to buy new licenses.

1. Expand the required recording server, right-click the hardware you want to replace.
2. Select **Replace Hardware**.
3. The **Replace Hardware** wizard appears. Click **Next**.
4. In the wizard, in the **Address** field (marked by red arrow in the image), enter the IP address of the new hardware. If known, select the relevant driver from the **Hardware Driver** drop-down list. Otherwise select **Auto Detect**. If port, user name or password data is different for the new hardware, correct this **before starting the auto detect process (if needed)**.

The wizard is prefilled with data from the existing hardware. If you replace it with a similar hardware device, you can reuse some of this data - for example, port and driver information.

5. Do one of the following:
 - If you selected the required hardware device driver directly from the list, click **Next**.
 - If you selected **Auto Detect** in the list, click **Auto Detect**, wait for this process to be successful (marked by a  to the far left), click **Next**.

This step is designed to help you map devices and their databases, depending on the number of individual cameras, microphones, inputs, outputs and so on attached to the old hardware device and the new respectively.

It is important to consider **how** to map databases from the old hardware device to databases of the new hardware device. You do the actual mapping of individual devices by selecting a corresponding camera, microphone, input, output or **None** in the right-side column.

Important: Make sure to map **all** cameras, microphones, inputs, outputs, etc. Contents mapped to None, are **lost**.

Click **Next**.

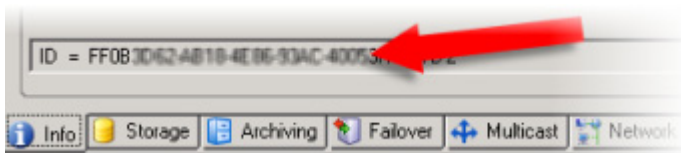
6. You are presented with a list of hardware to be added, replaced or removed. Click **Confirm**.

7. Final step is a summary of added, replaced and inherited devices and their settings. Click *Copy to Clipboard* to copy contents to the Windows clipboard or/and *Close* to end the wizard.

Replace a recording server

If a recording server is malfunctioning and you want to replace it with a new server that inherits the settings of the old recording server:

1. Retrieve the recording server ID from the old recording server:
 - a) Select *Recording Servers*, then in the **Overview** pane select the old recording server.
 - b) Select the *Storage* tab.
 - c) Press and hold down the CTRL key on your keyboard while selecting the *Info* tab.
 - d) Copy the recording server ID-number in the lower part of the *Info* tab. Do not copy the term *ID*, only the number itself.



2. Replace the recording server ID on the new recording server:
 - a) Stop the Recording Server service on the old recording server, then in Windows' *Services* set the service's *Startup type* to *Disabled*.

It is very important that you do not start two recording servers with identical IDs at the same time.
 - b) On the new recording server, open an explorer and go to *C:\ProgramData\OnSSI\Recording Server* or the path where your recording server is located.
 - c) Open the file *RecorderConfig.xml*.
 - d) Delete the ID stated in between the tags *<id>* and *</id>*.

```

- <recorderconfig>
- <recorder>
  <id>ff0b3d62-4b1b-4e86-93ac-400537482</id>

```

- e) Paste the copied recording server ID in between the tags *<id>* and *</id>*. Save the *RecorderConfig.xml* file.
- f) Go to the registry: *HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VideoOS\Recorder\Installation*.
- g) Open **RecorderIDOnMachine** and change the old recording server ID with the new ID.
- h) Restart the Recording Server service. When the new Recording Server service starts up, it has inherited all settings from the old recording server.

Video device drivers

About video device drivers

Your system uses video device drivers to control and communicate with the camera devices connected to a recording server. You must install video device drivers on each recording server on your system.

When you install your system, video device drivers are part of the initial installation process. OnSSI releases new versions of video device drivers, known as <DP>, from time to time and make them available for free on the OnSSI website. When you update video device drivers, you can install the latest version on top of any version you may have installed. Stop the Recording Server before you install, otherwise you need to restart the computer.

To ensure best performance, always use the latest version of video device drivers.

About removing video device drivers

If you no longer require video device drivers on your computer, you can delete the device packs from your system. To do so, follow the standard Windows procedure for removing programs.

If you remove video device drivers, the recording server and the camera devices cannot communicate any longer. Do not remove device packs when you upgrade because you can install a new version on top of an old one. Only if you uninstall the entire system, you may remove the device pack.

Services

About the Management Server service and Recording Server service

You can check the state of the Management Server service or the Recording Server service by looking at the icon in the notification area of the computer running the management server or recording server.

In the notification area, you can start and stop the Management Server service/Recording Server service, view status messages, check version information and more. To do this, right-click the server service icon. Depending on server type, select the needed icon. If you use multiple instances of the Recording Server service, you select a particular instance or all instances from a sub-menu.

If you stop the recording server service at some point, your system cannot interact with devices connected to the recording server. This means you cannot view live video or record video. If you stop the management server service, you cannot use the Management Client at all.

Important: When the **Recording Server service** is running, it is very important that Windows Explorer or other programs do not access Media Database files or folders associated with your system setup. If they do, the recording server might not be able to rename or move relevant media files, which might bring the recording server to a halt. If this situation has already occurred, stop the Recording Server service, close the program accessing the relevant media file(s) or folder(s), and restart the Recording Server service.

View status messages
















1. Right-click the notification area's server service icon.
2. Depending on server type, select the relevant icon.
3. Select *Show Status Messages*. Depending on the current server type, either the *Management Server Status Messages* or *Recording Server Status Messages* window appears, listing time-stamped status messages:



Example from Management Server service

Read server service icons - management, recording and failover

The following notification area icons represent the possible states of the Management Server service, Recording Server and Failover Recording Server services. They are all visible on the computers where the service is installed, not in the Management Client:

Management Server service icon	Recording Server service icon	Failover Recording Server service icon	Description
			Running. Reg. failover recording server, it is enabled and started and can take over from standard recording servers.
			Stopped. Reg. failover recording server, it is stopped and no longer taking over from standard recording servers.
			Starting. Appears when a server service is in the process of starting. Under normal circumstances, the icon changes after a short while to Running .
		Management and Recording Server service only	Stopping. Appears when a server service is in the process of stopping. Under normal circumstances, the icon changes after a short while to Stopped .
Recording Server service only		Recording Server service only	In indeterminate state. Appears when the Recording Server service is initially loaded and until the first information is received, upon which the icon, under normal circumstances, changes to Starting and afterwards to Running .
			Running offline. Typically appears when the Recording Server or Failover recording service is running but the Management Server service is not.
		Recording Server service only	Must be authorized by administrator. Appears when the Recording Server service is loaded for the first time. Administrators authorize the recording server through the Management Client: Expand the Servers list, select the Recording Server node and in the Overview pane, right-click the relevant recording server and select Authorize Recording Server .

Change recording server settings

To change basic settings for the Recording Server service, such as which port numbers to use:

You must stop the Recording Server service to change settings. While the Recording Server service is stopped, the system cannot interact with devices connected to the recording server. This means you cannot view live video or record video.

1. Right-click the server service icon.
2. Depending on server type, select the needed icon.
3. Select *Stop Recording Server service*.

4. Right-click the notification area's recording server icon.
5. Select *Change Settings*. The *Recording Server Settings* window appears. Change the appropriate settings.

Recording server properties

When you configure Recording server settings, specify the following:

Name	Description
Address	IP address (example: 123.123.123.123) or host name (example: ourserver) of the management server to which the recording server should be connected. This information is necessary so that the recording server can communicate with the management server.
Port	Port number to be used when communicating with the management server. Default is port 9993. You can change this if you need to.
Web server port	Port number to be used for handling web server requests, for example for handling PTZ camera control commands and for browse and live requests from Ocularis Client. Default is port 7563. You can change this if you need to.
Alert server port	Port number to be used when the recording server listens for TCP information (some devices use TCP for sending event messages). Default is port 5432. You can change this if you need to.
SMTP server port	Port number to be used when the recording server listens for Simple Mail Transfer Protocol (SMTP) information. Also, some devices use SMTP (e-mail) for sending event messages and/or for sending images to the surveillance system server via e-mail. SMTP is a standard for sending e-mail messages between servers. Default is port 25. You can change this if you need to.
FTP server port	Port number to be used when the recording server listens for FTP information (some devices use FTP for sending event messages). Default is port 21. You can change this if you need to.

Registered services

Occasionally, you have servers and/or services which should be able to communicate with the system even if they are not directly part of the system. Some services, but not all, can register themselves automatically in the system. Services that can automatically be registered are:

- Log Server service
- Service Channel service

Automatically registered services are displayed in the list of registered services.

You can manually specify servers/services as registered services in the Management Client.

About the service channel

The service channel enables automatic and transparent configuration communication between servers and clients in your system. For example, it is the service channel that makes sure that when a shared view is changed on one client, the change is immediately reflected on other clients using the relevant shared view. The service channel also facilitates configuration-related communication between servers and clients in cases where you use various plug-ins or add-on products with your system.

The service channel is typically installed as part of the management server installation and resides on the management server computer, but if needed, you may just as well install it on another server in your surveillance system.

Once installed, the service channel can register itself automatically with your system (meaning that it automatically becomes listed by the registered services feature in the Management Client). Its location is known by the system, and clients logging into the system can automatically benefit from it.

If you later change the IP address or hostname of the server running the service channel service, you must manually edit the information under *Tool > Registered Services* in the Management Client. Also, if you later need to change the user under which the service channel service was installed, you must remove the Service Channel service and afterwards install it again under the new user.

It is important that any instance of Ocularis Client is time-synchronized with the computer running the Service Channel service. If an Ocularis Client is not time-synchronized with the management server and the computer running the Service Channel service, the Ocularis Client is not updated with information about configuration changes made by other users in Ocularis Client. This means that users risk overwriting each others' configuration changes. If your Ocularis Clients are not time-synchronized with the computer running the Service Channel service, you see an error informing you of this.

Add and edit registered services

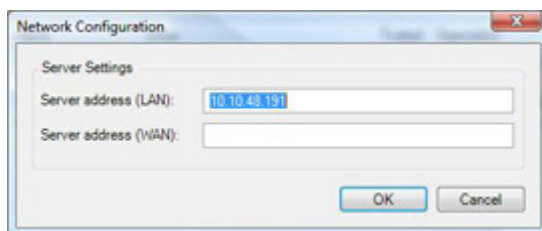
1. In the *Add/Remove Registered Services* window, click *Add* or *Edit*, depending on your needs.
2. In the *Add Registered Service* or *Edit Registered Service* window (depending on your earlier selection), specify or edit settings.
3. Click *OK*.

Manage network configuration

With the network configuration settings, you can specify the management server's server LAN and WAN addresses so the management server and the trusted servers can communicate.

1. In the *Add/Remove Registered Services* window, click *Network*.
2. Specify the LAN and/or WAN IP address of the management server.

If all involved servers (both the management server and the trusted servers or the required Ocularis CS) are on your local network, you can simply specify the LAN address. If one or more involved servers access the system through an internet connection, you must also specify the WAN address.



3. Click *OK*.

Registered services properties

In the *Add Registered Service* or *Edit Registered Service* window, specify the following:

Component	Requirement
Type	Prefilled field.
Name	Name of the registered service. The name is only used for display purposes in the Management Client.
URLs	<p>Click <i>Add</i> to add the IP address or hostname of the registered service. If specifying a hostname as part of a URL, the host must exist and be available on the network. URLs must begin with <i>http://</i> or <i>https://</i> and must not contain any of the following characters: <code>< > & ' " * ? []</code>.</p> <p>Example of a typical URL format: <i>http://ipaddress:port/directory</i> (where port and directory are optional). Note that you can add more than one URL if required.</p>
Trusted	<p>Select if the registered service should be trusted immediately (this is often the case, but the option gives you the flexibility to add the registered service and then mark it as trusted by editing the registered service later).</p> <p>Note that changing the trusted state also changes the state of other registered services sharing one or more of the URLs defined for the relevant registered service.</p>
Description	Description of the registered service. The description is only used for display purposes in the Management Client.
Advanced	When a service is advanced, it has specific URI schemes (for example, <i>http</i> , <i>https</i> , <i>tcp</i> or <i>udp</i>) that need to be set up for each host address you define. A host address therefore has multiple endpoints, each with its own scheme, host address and IP port for that scheme.

Index

3

360° Lens tab (devices) • 69

A

About actions and stop actions • 64, 82

About archive structure • 40

About back up/restore fail and problem scenarios • 155

About backing up and restoring your system configuration • 28, 154

About basic users • 120

About camera devices • 23, 54

About camera settings • 60

About clients • 77

About configuration reports • 122

About current tasks • 122

About day length time profiles • 97, 99

About daylight saving time • 26

About default rules • 92

About device groups • 52

About devices • 52, 54

About dynamic sensitivity • 75

About failover recording server functionality • 133

About failover recording server services • 137

About failover recording servers • 42, 91, 131

About failover steps • 132

About generate motion data for smart search • 76

About hardware • 45

About input devices • 56

About Interconnect • 147

About licenses • 13

About local IP address ranges • 14

About login authorization • 27

About logs • 123, 128

About Management Client profiles • 78, 104

About manually backing up your system configuration • 155

About metadata devices • 56

About microphone devices • 55

About moving the management server • 158

About multicasting • 42, 71

About multiple management servers (clustering) • 138

About multi-streaming • 60, 61

About NetMatrix • 80

About notification profiles • 100, 129

About Ocularis Client • 11

About Ocularis CS servers • 120, 151

About Ocularis Mobile • 11

About Ocularis Web • 12

About OnSSI Federated Architecture • 120, 142

About output devices • 57

About possible Interconnect setups • 148

About pre-buffering • 63

About recording servers • 33

About remote connect services • 140

About remote recording • 65

About removing video device drivers • 162

About rights of a role • 104

About roles • 23, 104

About rule complexity • 94

- About rules • 91
- About rules and events • 23, 81
- About scheduled backup and restore of system configuration • 156
- About selecting Interconnect or OnSSI Federated Architecture • 142, 146
- About SNMP support • 150
- About speaker devices • 55
- About storage • 64
- About storage and archiving • 23, 36, 65
- About system dashboard • 121
- About system monitor • 121
- About the Client tab • 70
- About the Events tab • 69
- About the Info tab • 60
- About the Management Client • 11
- About the Management Server service and Recording Server service • 157, 162
- About the Motion tab • 74
- About the Patrolling tab • 67
- About the Presets tab • 65
- About the Privacy Mask tab • 71
- About the Record tab • 62
- About the service channel • 29, 164
- About the Settings tab • 60
- About the Streams tab • 61
- About time profiles • 97
- About time servers • 27
- About unavailable management servers • 158, 159
- About updating the SQL server address • 159
- About upgrade • 15, 24
- About user-defined events • 90, 103
- About validating rules • 93
- About video device drivers • 161
- About view groups • 77
- About view groups and roles • 77
- About virus scanning • 17
- Accept inclusion in hierarchy • 144
- Activate input manually for test • 57
- Activate licenses after grace period • 32
- Activate licenses offline • 23, 31, 158
- Activate licenses online • 23, 31
- Activate output manually for test • 57
- Active Directory • 10, 16
- Add a configuration report • 122
- Add a device group • 53
- Add a new storage • 38
- Add a patrolling profile • 49, 67
- Add a preset position (type 1) • 49, 65
- Add a rule • 94
- Add a stream • 61
- Add a user-defined event • 103
- Add a view group • 77
- Add an event • 69
- Add and configure a Management Client profile • 78
- Add and edit registered services • 165
- Add and manage a role • 104
- Add hardware • 23, 45, 148
- Add NetMatrix recipients • 81
- Add notification profiles • 100
- Add Ocularis CS servers • 151, 152

Add site to hierarchy • 144

Add/edit STSs • 140

Alternative upgrade for workgroup • 20, 25

Archive settings properties • 23, 38

Assign a default preset position • 66

Assign failover recording servers • 134

Assign IP address range • 43

Assign local IP ranges • 44

Assign/remove users and groups to/from roles • 23,
104, 105

Attach a device or group of devices to a storage • 23,
36, 39

Audit log properties • 125

Authorize a recording server • 23, 33

AVI Generation tab (options) • 127, 129

Axis One-Click Camera connection properties • 141

B

Back up archived recordings • 40

Back up log server database • 155, 158

Back up system configuration manually • 155

Back up system configuration with scheduled backup
• 157, 159

Backing up and restoring configuration • 40, 154

Basic users • 120

Basics • 30

Before you start • 8

Best practices • 26

C

Change log language • 124

Change recording server settings • 163

Change Software License Code • 23

Change the management server address • 137

Change/verify the basic configuration of a recording
server • 34

Client • 77

Client tab (devices) • 70

Client tab properties • 71

Clients • 11

Configure report details • 123

Configure SNMP service • 151

Configure the system in Management Client • 18, 20,
22

Connect to another site in hierarchy • 145

Copy a Management Client profile • 78

Copy, rename or delete a role • 105

Copyright, trademarks and disclaimer • 7

Create a day length time profile • 99

Create an archive within a storage • 38

Create basic users • 107, 121

Customize IIS • 16

Customize transitions • 67

D

Day length time profile properties • 99

Deactivate and activate a rule • 96

Define public address and port • 44

Define roles with access to Ocularis CS servers • 151,
152

Define rules sending video to NetMatrix recipients •
81

Delete all hardware on a recording server • 51

Delete an archive from a storage area • 41

Delete an entire storage area • 41

Detach a site from the hierarchy • 145

Determine installation method • 15

Determine SQL server type • 15

Device tab (roles) • 116

Devices • 52

Devices which require a license • 30

Differentiate LS and ES Recorders • 13, 41, 104, 140, 150

Disable/enable hardware • 46

E

Edit a preset position (type 1 only) • 66

Edit a time profile • 98

Edit basic hardware settings • 47

Edit Ocularis CS servers • 151, 152

Edit settings for a selected storage or archive • 39

Edit, copy and rename a rule • 96

Enable and disable motion detection • 74

Enable keyframe recording • 64

Enable manual sensitivity • 75

Enable multicasting • 43

Enable multicasting for individual cameras • 44

Enable playback directly from remote site camera • 62, 149

Enable PTZ on a video encoder • 49

Enable recording on related devices • 62, 70

Enable/disable devices via device groups • 54, 55, 56, 57, 58

Enable/disable individual devices • 47

Enable/disable privacy masking • 72

Enable/disable recording • 62

Establish remote desktop connection to remote system • 149

Event tab (properties) • 70

Events overview • 87

Events tab (devices) • 55, 57, 69

Events tab (remote server) • 50

Export logs • 124

External Event tab (roles) • 119

F

Failover group properties • 136

Failover management server • 9

Failover management servers • 138

Failover recording server • 10

Failover recording server properties • 136

Failover recording servers (regular and hot standby) • 131

Failover tab (recording server) • 41

Failover tab properties • 42

Feature configuration • 8, 131

Federated site properties • 146

First time use • 8, 26

Flush SQL server transaction log • 157

G

General tab • 146

General tab (options) • 127

Get additional licenses • 31, 32

Group failover recording servers • 135

H

Hard disk failure

protect your drives • 26

Hardware and remote servers • 45

I

Info tab (devices) • 55, 56, 57, 60

Info tab (hardware) • 47

Info tab (Management Client Profiles) • 78

Info tab (recording server) • 35

Info tab (remote server) • 47, 49

Info tab (roles) • 78, 106

Info tab properties • 35, 60

Install a failover recording server • 20, 133

Install in a cluster • 138, 140

Install SNMP service • 151

Install STS environment for One-click camera connection • 140

Install the recording server • 18, 19, 20

Install the system • 17, 22, 25

Install your system - Custom option • 17, 19

Install your system - Distributed option • 17, 18

Install your system - Single Server option • 17, 18

Installation • 8, 15

Installation for workgroups • 16, 20, 25

Installation preconditions • 15

Installation troubleshooting • 21

Interconnect • 146

Interconnect and licensing • 148

Introduction to Online help • 8

Issue

Automatic installation of IIS failed • 21

Changes to SQL server location prevents database access • 22

Recording server startup fails due to port conflict • 21

L

License information • 30

On-Net Surveillance Systems, Inc.

Licenses and hardware device replacement • 32

Log server • 10

M

Mail Server tab (options) • 127, 129

Manage hardware • 47

Manage manual recording • 63

Manage network configuration • 165

Manage pre-buffering • 63

Manage remote servers • 49

Management Client elements • 8, 29, 30

Management Client overview • 11, 27

Management Client profile properties • 78

Management Client profiles • 78

Management Client window • 27

Management server • 9

Managing the SQL server • 159

Manual backup and restore • 155, 156

Menu overview • 28

Motion tab (devices) • 55, 74

Move non-archived recordings from one storage to another • 41

Move the system configuration • 159

Moving the management server • 158

Multicast tab (recording server) • 42

Multi-domain with one-way trust • 150

N

Navigate the built-in help system • 8

NetMatrix • 80

NetMatrix tab (roles) • 120

Network tab (options) • 127, 130

Network tab (recording server) • 44

Notification profile (properties) • 101

Notification profiles • 100

O

Ocularis CS servers • 151

OnSSI Federated Architecture • 142

Options dialog box • 126

Overall Security tab (roles) • 78, 107

P

Panes overview • 27

Parent Site tab • 146

Patrolling tab (devices) • 67

Ports used by the system • 153

Power outages

 use a UPS • 26

Prerequisites • 100

Prerequisites for clustering • 138

Presets tab (devices) • 65

Privacy mask tab (devices) • 71

Privacy mask tab (properties) • 73

Product overview • 9

Profile tab (Management Client Profiles) • 79

Protect recording databases from corruption • 26, 34

PTZ tab (roles) • 118

PTZ tab (video encoders) • 48

R

Read failover recording server status icons • 136

Read server service icons - management, recording
 and failover • 163

Record tab (devices) • 55, 56, 62

Recorder downloads web page • 24

Recording server • 9

Recording server properties • 164

Recording server status icons • 34

Recording servers • 33

Refresh site hierarchy • 145

Register new Axis One-click camera • 141

Registered services • 164

Registered services properties • 166

Remote connect services • 140

Remote Recordings tab (roles) • 119

Remote Retrieval tab • 51

Remove a recording server • 51

Rename a user-defined event • 103

Replace a recording server • 161

Replace hardware • 32, 160

Restart Data Collector Server service • 122

Restore system configuration from manual back up •
 155

Restore system configuration from scheduled backup
 • 157, 159

Retrieve remote recordings from remote site camera •
 149

Roles • 104

Roles settings • 106

Rule log properties • 126

Rules • 91

Rules and events • 81

S

Scheduled backup and restore • 156

Search logs • 124

Security • 104

Select image processing interval • 76

- Select keyframes settings • 75
- Select service account • 16
- Select shared backup folder • 156
- Server logs • 123
- Server Logs tab (options) • 123, 127, 128
- Servers and hardware • 33
- Servers tab (roles) • 120
- Services • 162
- Set up a secure connection to the hardware • 47
- Set up your system to run federated sites • 143
- Settings tab (devices) • 55, 56, 57, 60
- Settings tab (hardware) • 48
- Settings tab (remote server) • 48, 50
- Setup and enable failover recording servers • 134
- Setup with one-way trust • 150
- Site information • 32
- SNMP • 150
- Specify a time profile • 97
- Specify an end position • 68
- Specify common properties for all devices in a device group • 53, 54
- Specify datagram options • 43
- Specify detection method • 76
- Specify event properties • 69, 70
- Specify exclude regions • 76
- Specify manual PTZ session timeout • 68
- Specify motion detection settings • 74, 75
- Specify preset positions in a patrolling profile • 67
- Specify privacy mask settings • 72
- Specify recording frame rate • 64
- Specify the time at each preset position • 67
- Specify threshold • 75
- Specify which devices to include in a device group • 53
- Speech tab (roles) • 119
- SQL server • 10
- Status icons of devices • 59
- Storage tab (recording server) • 35
- Streams tab (devices) • 55, 61
- System components • 9
- System dashboard • 121
- System log properties • 124
- System maintenance • 8, 153
- System overview • 8, 9
- System requirements • 14
- T**
- Test a preset position (type 1 only) • 66
- Time profiles • 97
- U**
- Update remote site hardware • 148
- Update site information • 32
- Update the log server's SQL address • 159
- Upgrade • 24
- Upgrade in a cluster • 139
- Upgrade prerequisites • 25
- Use preset positions from the camera (type 2) • 65
- Use rules to trigger email notifications • 101, 129
- Use several instances of an event • 69, 70
- User and Groups tab (roles) • 107, 120
- User Settings tab (options) • 127, 130
- User-defined events • 103

V

Video device drivers • 161

View effective roles • 106

View Group tab (roles) • 120

View groups • 77

View license overview • 31

View status messages • 137, 162

View version information • 137

Virtual servers • 10

W

Why use a public address? • 44

Windows Task Manager

 be careful when you end processes • 26

Working with device groups • 52

Working with devices • 23, 54